Received Comments on SP 800-131: Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

David J. Cornwell, Coact....2
Scott Judy....3
Malcolm Levy, Checkpoint....4
Travis Spann, ÆGISOLVE....6
Apostol Vassilev, ATSEC....8
William Gill, EPA....10
Jason Soter, U.S. Army....12
Michael.Vogel, Giesecke & Devrient....13
Andras Szakal, IBM....15
Lovell King II, State....17
Timothy Fong, DOD....18
Stephen Savard, CSEC....22
Brian Weis, Cisco....23
Jan Hintermeister, Motorola....26
Auston Holt, ATSEC....28
James Knoke, Cygnacom....30
Nicky Tabram, Thales....32
Anthony Busciglio, Cisco....37
Vijay Bharadwaj, Microsoft....43
Santosh Chokhani, Cyganacom Solutions....44
Chris Brych, DOMUS IT Security Laboratory....46
Joan Lozano, Infogard....47
Andras Szakal, IBM (additional comments)....59
Joan Lozano, Infogard....61
Jonathon Shu, OSD....65
Miles Smid, Orion Security....74
Wade Hanniball, Digital Cinema Initiatives....76

From: David J. Cornwell [dcornwell@coact.com]

IG 7.2 refers to IEEE 802.11i Key Derivation Protocols.

This does not seem to be addressed in your Transitions Paper SP 800-131
Although other IGs and protocols are specifically referenced.

Please add a note to the paper SP 800 - 131 concerning the status of this protocol and its key derivation functions. This is used by one of our most important vendors and questions concerning it are sure to come up.

Suppose I have a module I submit in 2011 but it uses CAVP algorithm
certificates for RNGs (non SP 800-90) which are dated 2010 or earlier.

Can this module claim them through 2015 or does the module need to implement SP 800-90 RNGs and have them go through CAVP?

David Cornwell, CISSP
Sr. Security Analyst
COACT CAFE LAB
(301) 498 0150 TEL x210
(301) 498 0855 FAX

From: scottajudy@aol.com

1. What is the standard by which you determine what strength is adequate and what is not?
2. What projections do you make and how do you make them to ensure that the future dates that you set are reasonable and adequate?

While providing this rationale opens up a door for future speculation, simply putting marks in the sand without substantiating any of them is not a sound scientific principle.

Sincerely,
Scott Judy

From: Malcolm Levy [mlevy@checkpoint.com]

I'm writing regarding contradictory messages that I've received on the implementation plan for the transition of 800-131 as I need to understand this for crypto modules that I plan to certify in 2010.

The message I received from testing laboratories is that FIPS certificates will only be awarded for 2011 where the module is compliant with the draft 800-131 with the implication being that a module needs to have its lab report submitted by the end of May to take account of the queue which can take at least 5 months.

However the draft standard http://csrc.nist.gov/publications/drafts/800-131/draft-800-131_transition-paper.pdf states the following, which I read as saying that a new FIPS certificate under the current rules will be given as long as the lab report is presented before EOY.

1.2.4 New Validations and Already Validated Implementations
This Recommendation contains several tables addressing the implementation of cryptographic algorithms and modules. This includes both New Implementations and Already- Validated Implementations:

- New Implementations are the cryptographic algorithms or modules that are being tested by an accredited CST laboratory for which the test report has been submitted to CMVP under FIPS 140-2 Implementation Guidance G.8, Scenarios 3 and 5. The date in the table refers to the date of the lab's submission of the test report to the validation authorities.

Please clarify as this difference has very important implications on the ability to offer certified solutions within a reasonable time frame as required by Federal Agencies and the DoD.

I am very concerned as if the lab rumor is true the date by which I need to plan for a FIPS report to be submitted is very in-deterministic as I have no control over the queue or the length of time that the final negotiation with the Validators will take. As a Project Manager my control only extends to the evidence developer and lab resources which I have responsibility for engaging.

Another concern is that I have products undergoing Common Criteria evaluation and NIAP-CCEVS require a FIPS certificate before completion. If I wait till the 800-131 changes are merged into these products, it will not be possible to complete FIPS before CC as required by NIAP-CCEVS.

To meet commitments of CC and Federal Agencies (including the Army), I need to have the ability to certify current implementations with a plan to maintain these certificates in the next 12-18 months as new versions are released that are fully conformant and also take on board the ability to manage 'old' deployed modules which have not yet been updated to conform to the new standard.

Many thanks,
Malcolm

+972 545713450 (mobile)
+972 37534561 (office)
Check Point Certification Manager

From: Travis Spann [tspann@aegisolve.com]

The wording in the draft SP800-131 is slightly different than the discussion paper for The Transitioning of Cryptographic Algorithms and Key Sizes.

In particular the discussion paper was more explicit, and stated that the crypto module could not use SHA-1 for standalone hashing after 2010.

Transitioning_CryptoAlgos_070209.pdf
"When SHA-1 is used for hash-only applications, the use of already-validated implementations is disallowed after 2010 in the FIPS mode."

However, the draft SP800-131 is being interpreted by some vendors as allowing the use of SHA-1 as a standalone hashing function.

draft-800-131_transition-paper.pdf
"if a module contains both MD5 and SHA-1, then when hashing is required in the FIPS mode, SHA-1 must be used."

"[SHA-1] Approved for all non-digital signature generation applications"*

Note that there is an asterisk after the statement…but there is no clarification/footnote about what this means (i.e. purpose of asterisk is undefined)

How is this to be interpreted? Can SHA-1 be used in FIPS mode for stand alone hashing (not within signatures, MACs, KDF, etc.) after 2010?

- It is unclear whether the SP800-131 disallows the use of SHA-1 as a standalone hash function. The prior NIST discussion paper stated that "When SHA-1 is used for hashonly applications, the use of already-validated implementations is disallowed after 2010 in the FIPS mode." However, this statement was not included in the SP800-131.

- There is a asterisk (*) in the column next to SHA-1 in Table 9 that does not seem to be defined or associated with any footnote.

- The statement that "if a module contains both MD5 and SHA-1, then when hashing is required in the FIPS mode, SHA-1 must be used" may seem to recommend SHA-1 as the hashing function of choice…

- It is unclear whether TLS using the RSA for key transport will be allowed after 2013. Is the plan to update the IG D.2 to state that untested TLS scheme with 2048+ bit keys will not be allowed after 2013?

Section 5.2 and Table 5 say that the KDFs used in the legacy protocols listed in IG D.2 are allowed (with no mention of any expiration). However, in IG D.2, the KDFs in some of the protocols listed there, including SSH, are specifically fused to terminate at Dec 2010 right there in the IG document. This seems to conflict with SP800-131.

Is the plan to update the IG D.2 to clarify that KDFs (including SSH) can be used for an extended period of time beyond Dec 2010?

Thanks,

Travis Spann - President, Laboratory Director
ÆGISOLVE, INC.
1400 Railroad St. Ste: 101
Paso Robles, CA. 93446
805.239.2043 tel
805.239.1743 fax
aegisolve.com

From: Apostol Vassilev [apostol@atsec.com]

The Draft SP 800-131 has generated a lot of rumors in the industry about the fate of TLS 1.2, most of which I find contradictory to the guidelines provided in the paper. The biggest concerns come from sun-setting SHA1 for signature generation and people are afraid that relatively older certified implementations of modules with TLS 1.2 in them will become invalid at the end of this year. Please note that this question is independent of the concerns about the protocol fixes for the session renegotiation vulnerability discovered recently.

I would like to confirm my understanding so I can answer my customer's questions before they go out and develop new products. I consulted also Elaine's presentation from the December 2009 Lab Managers meeting.

Is TLS 1.2 going to be allowed in FIPS-mode for already validated implementation starting in 2011, so previously certified modules will retain their certificates when TLS 1.2 is used? If so, for what purposes can TLS 1.2 be used as an allowed algorithm while the module is running in FIPS-mode?

Please provide some guidance. Thanks.

--
Apostol Vassilev
Manager - Cryptographic and Security Testing Laboratory
NVLAP Accreditation 200658-0: CMVP, CAVP, NPIVP, SCAP, GSA FIPS 201 EP
atsec information security, 9130 Jollyville Rd. #260, Austin, TX 78759
Tel: +1.512.615.7339, Fax: +1.512.615.7301, Web: www atsec com

From: Apostol Vassilev [apostol@atsec.com]

Reading SP 800-131, I find the following statement:

"Protocols are used for a very long time. When new versions of a protocol are designed and implemented, a module may need to include a capability to interoperate with both the new and existing protocols. Because of this, the KDFs in those existing protocols will continue to be allowed. NIST will encourage the adoption of KDFs that are approved for key agreement, such as those specified in SP 800-56A, for new and revised protocols."

Furthermore, Table 5, in the next-to-last row states that KDFs in protocols listed in IG D.2 will be allowed for New and Already Implemented Validations.

However, when it comes to TLS, IG D.2, p.112 states that a KDF may conform to the TLS KDF but only to December 31, 2010.

To contrast this with key transport, IG D.2, p. 113, states that the key transport scheme of TLS may be used in FIPS mode.

Am I reading this right? Is the KDF for all TLS versions going out of service for FIPS at the end of this year? Is it really the intent to allow key transport with TLS but disallow KDF? Please let me know how to interpret this.

Thanks.

--
Apostol

From: Gill.William@epamail.epa.gov

I have attached a document with screen shots of my smart card certificate. This was recently (fall of 2009) updated to allow use wiith OMB's "CyberScope" FISMA Reporting application.

According to your presentation (slide 6), the transition will make certain Digital Signatures invalid beginning 2011. It appears the Cert. (from the ORC service provider) on my card will be valid re: the requirement to use RSA >= 2048 bits and a signiture verification >= 80 bits. However, the highlighted section which states invalidation of implementations of RSA that only use SHA-1 for Dig sig generation.

See arrows on the enclosed document. Of note is the thumbprint algorithm using "sha1" and the signature algorithm "sha1RSA." This would appear to fit into the invalidation criteria range. Could you or one of your coworkers validate that this is correct. If you need additional information let me know. Note these certificates are supposed to be "valid" until 3/18/2012.

I would like some expert opinion on this before I contact our smartcard folks in physical security as we are nearing completion of issuing over 19K smart cards with several thousand updates to allow logical access.

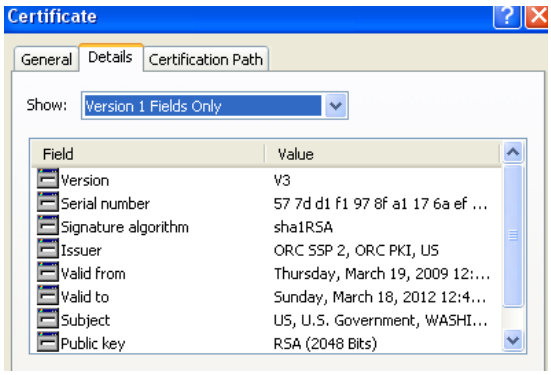
Thank you for your assistance.

(See attached file: Good-orBad-CERT.doc)

William Gill, CISSP
Technology and Information Security Staff
Office of Technology Operations and Planning
Office of Environmental Information
Environmental Protection Agency
202-566-0348

Certificate

Field	Value
Version	V.3
Serial number	577D D1F1 978F A117 6AEF 3DA0 F
Signature algorithm	sha1RSA
Issuer	CN=ORC SSP 2,O=ORC PKI,C=US
Valid from	03/19/2009
Valid to	03/18/2012
Common name	WILLIAM A. GILL
Organizational unit	WASHINGTON
Organization	U.S. Government
Country	US
Public key	3082 010A 0282 0101 00A7 EC6F A
Authority Key Identifier	KeyID=7a e8 df 1a e0 ac 51 22 ca a
Enhanced Key Usage	Any Extended Key Usage (2.5.29.3
Key Usage	Digital Signature(80)
Authority Information Access	[1]Authority Information Access:,
Certificate Policies	[1]Certificate Policy:, PolicyIdent
CRL Distribution Points	[1]CRL Distribution Point, Distribu
Subject Alternative Name	Other Name: , FASC-N=d3 44 10
NACI Status	Completed
Subject Key Identifier	cf 63 ae ae 9e d3 e2 e7 2d 18 b8 61
Subject	C=US,O=U.S. Government,OU=WA
Thumbprint	4C4C EB9D A4EB 3064 F99B 5E93 3
Thumbprint Algorithm	sha1



From: Soter, Jason [jason.j.soter@us.army.mil]

Will there be any type of "grandfathering" or extension granted to those systems that are currently in the process of receiving certification at the 80 bits (Two key triple DES)? We are currently in the process of being granted FIPS 140 2 Level 1 & 2 certification but in light of what has been stated in the DRAFT report that certification will only be good for several months and will expire on 31 DEC 10.

Thank you,
Jason Soter
703-704-3553

From: Michael.Vogel@gi-de.com

Please find enclosed some minor comments on the Transitioning Guide SP 800-131 from Giesecke & Devrient from a Smart Card vendor's point of view.

1.) Chap. 4: Note 'a' for Table 3 states that implementations of the RNG in ANS X9.31 that use two-key TDES will continue to be approved through 2015. Does this also hold for RNGs according to SP800-90 using two key TDES? If so, it should also be mentioned/clarified in chap. 4.

2.) General remark on RSA keylengths. A change to 2048 Bit keys seems to be reasonable for RSA. For smart card APDU based communication without command chaining/extended length 256 Byte are the limit in length for commands and responses. Due to the overhead in command/response structure and the application of Secure Messaging algorithms for secure communication the key sizes are limited for some use cases to values just below 2048 Bit. For example in the German scheme for qualified electronic signatures (which are more or less legally binding as hand-written signatures) a key length of 2048 bit is recommended but a minimum key length of 1976 Bit is required due to the restrictions on command/response lengths explained above (official algorithm catalogue attached - see chap. 3.1, unfortunately available in German only, can be obtained through http://www.bundesnetzagentur.de/media/archive/18226.pdf). We therefore suggest a note that allows slightly lower key lengths than 2048 bit for RSA if required as an exception to the rule.

3.) As of December 31, 2010 some algorithms and key sizes will no longer be approved for use by the Federal government.
Previously issued CMVP certificates will have to be modified to remove them from the approved list for the FIPS mode.
If the cryptographic module includes at least one approved algorithm for the FIPS mode (e.g., AES, RSA 2048, SHA-256), the previoulsy issued CMVP certificate for that module shall not become entirely invalid.
In case you plan to invalidate the entire certificate, even though it still includes approved algorithms (e.g., AES with approved key sizes), it would be good to have an extended deadline of 6-9 months after December 31, 2010.

In case you have any questions please feel free to contact me.

Kind regards,

Michael Vogel

Dr. Michael Vogel
Technology Consulting / Department CSRD22
Giesecke&Devrient GmbH,Prinzregentenstraße 159, D-81677 Munich
Tel.: 089/4119-2961, FAX: 089/4119-2819

mailto:Michael.Vogel@gi-de.com
http://www.gi-de.com

From: Andras Szakal [aszakal@us.ibm.com]

I am providing the following comments on 800-131 on behalf of IBM Software Group. Additional comments from our systems division may be pending.

While IBM certainly understands and agrees with the desire to move to larger and more secure cryptographic strengths. However, we have some concerns about the time frames as outlined in the current draft of 800-131. This is especially true for the move from SHA1 to SHA2 and the subsequent need to move from the widely adopted Secure Sockets / SSL 3.0 (or TLS 1.0) to TLS 1.2.

Consider that remediation of our products to comply with this new standard requires a 5 step process;

I. Updating existing cryptographic modules,
II. Evaluation of the modules under FIPS 140-2,
III. Updating the secure sockets SDKs and run-times to support TLS 1.2 and the new ciphersuites,
IV. Re-valuation of the secure sockets SDKs and run-times under the Common Criteria, and
V. Finally, upgrading the products to use the new security providers at the appropriate new levels.

The adoption process can not realistically start for 800-131 until all comments have been received in March and the final guidance published and the standard is stable. Once product remediation is complete, the external certification lab testing of a month or 2 and normal NIST CMVP certification cycle of approximately 6 to 8 months, may begin. This is then followed by the many IBM products and applications coding to the new provider and rules followed by distribution to our many customers.

Thus a more realistic goal for changed and certified Security providers of 2Q 2011 and compliance/usage by appropriate IBM products of 4Q 2011 is respectfully recommended.

Please note that our lead crypto engineer, Tom Benjamin, is working overtime to effectively position IBM SWG to comply with these changes. Internally, we have discussed the suggested changes and agree they will provide significant additional protection to our customers. However, please consider that we manage thousands of products that will need remediation. This is not an insignificant change. We are assuming similar challenges for other vendors. As such we also recommend a period of phased transition for adopting 800-131.

Regards,
Andras

Andras Robert Szakal, CSSLP
IBM DE, Director Software Architecture
US Federal Software Group

Member Open Group Board of Directors
Tie Line: 518-3279
External Line/fax: 703-943-3279
email: aszakal@us.ibm.com

From: King II, Lovell [KingL@state.gov]

The U.S. Department of State concurs with the proposed draft without comment.

Thank you.

…Lovell

Lovell King II
Senior Analyst
U.S. Dept. of State - IRM/IA
phone: (703) 812-2428
fax: (703) 812-2547

From: Fong, Timothy [Timothy.Fong@osd.mil]

MEMORANDUM FOR U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, COMPUTER SECURITY DIVISION

Subject: Department of Defense Response to Draft NIST Special Publication 800-131

The Department of Defense (DoD) fully supports the need to transition to stronger cryptography and DoD is working aggressively to migrate to stronger cryptographic algorithms and key sizes. Moreover, the DoD is also a strong advocate for the use of PKI and energetically embraced the technology and associated policy requirements. PKI technology is now deeply embedded in the DoD's networks and business processes, making the transition proposed in Draft NIST SP 800-131 unrealistic with the proposed timelines (Jan. 2011). Due to the DoD's diverse and globally deployed infrastructure supporting and interfacing with PKI credentials, the Department faces significant operational and fiscal challenges in transitioning to the SHA-256 cryptography as proposed. The Department has consistently voiced and continues to stress concerns regarding transitioning to larger key sizes and new cryptographic algorithms to the Office of Management and Budget (OMB) through the DoD's implementation plans for Homeland Security Presidential Directive 12 (HSPD-12).

In response to the forthcoming cryptography upgrades, the DoD has conducted limited testing and gathered data on commercially provided products, applications and devices that support the issuance and use of PKI credentials. The Department's initial findings indicate most products, applications, and devices are not in compliance with, nor have been tested, by NIST. Many vendors only recently began the process to incorporate support for the new requirements.

As a result, the Department will be unable to meet the proposed January 2011 transition date and nonconcurs with the Draft NIST SP 800-131 and recommends it be revised to reflect a technically and fiscally realistic date. More detailed observations are provided at the attachment. DoD recommends a date be established based on vendor product availability and normal federal technology refresh cycles. The DoD will provide NIST an integrated transition and acquisition strategy within the next nine months based on the results of our testing, vendor product availability, and technology refresh cycles.

Our lead for this effort is Mr. Robert "Scott" Jack, Director, Identity Assurance and Public Key Infrastructure (IdA/PKI) Directorate. He can be reached at,

Robert.Jack@osd.mil, (703) 604-5522, ext 101. Thank you for your attention and assistance with an effort that merits more government attention before it is implemented.

David M. Wennergren
DoD Deputy Chief Information Officer

Attachment:
DoD General Observation on Draft NIST SP 800-131

DoD General Observation on Draft NIST SP 800-131

- DoD fully understands and supports the need to migrate to stronger cryptographic keys and more robust algorithms but disagrees with NIST's recommended timeline for implementation.

- DoD disagrees with NIST's recommendation that the Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) should review, modify, and/or revoke the accreditation certificates for already validated products and implementations which are currently valid beyond December 31, 2010.

- DoD believes the better approach is to incorporate new algorithms into protocols that permit negotiation to the strongest, mutually acceptable algorithm, while allowing legacy products to work for a reasonable period of time. This permits early use of newer algorithms when both ends have the appropriate software while not introducing interoperability problems for legacy systems.

- Large organizations, such as DoD, need several years to replace existing software throughout the agency. Practical considerations may require the DoD to continue to use existing products and implementations after December 31, 2010. This is due to the operational needs of the Warfighter at the edge and the millions of DoD active-duty, reserve, civilian, and contractor personnel the Warfighter depend on for real-time 24/7 support. The alternative of accelerating upgrades or replacements to legacy products has substantial financial costs and is fiscally infeasible.

- Results from the analysis conducted by DoD's Cryptographic Migration Team highlight that almost all of the 40 Certificate Authorities in use, their associated Hardware Security Modules, and the supporting card issuance infrastructures servicing over 15 million certificates cannot support the recommendations by the suggested deadlines. The DoD infrastructure utilizes and is dependent on commercial products that are not yet available or in compliance with the recommendations of SP800-131.

- Current FIPS 140-2 validated smart cards and applets support some of the stronger cryptographic algorithms and key sizes recommended by NIST SP 800-131. Some of these algorithms are not valid for all uses inside the card (for instance, smart cards that are fully compliant with Global Platform Card Specification 2.1.1 only accept the Secure Channel protocol based on 2TDEA cryptography). Invalidating some algorithms from the FIPS 140 approved list after December 31, 2010 would have a major effect on the DoD. The DoD would need to revoke and

re-issue over 3.6 million cards since the cards will no longer be running in a FIPS140 approved mode. Reissuing this number of cards in such a short period of time is not feasible.

If the DoD does not meet existing requirements defined in Sections 6.15 of the Certificate Policies for the Federal Bridge Certification Authority and the U.S. Federal PKI Common Policy Framework to transition to SHA-224/SHA-256 and AES by December 31, 2010, the DoD will have substantial interoperability issues with the Federal Bridge. If the NIST recommended transition timelines in current draft SP800-131 are approved, they many become additional policy requirements for the DoD.

From: Savard, Stephen M. [Stephen.Savard@cse-cst.gc.ca]

1) Is there a timeframe for removing SHA-1 from all applications?

2) Remove from the Table of Contents under section 7 the line " The GDOI protocol is listed as an allowed protocol in IG D.2"

3) Remove the underscore after shall not in the first paragraph on page 2.

4) In section 1.2.4, change "Already- Validated Implementations" by removing the space and making it "Already-Validated Implementations".

5) In the last paragraph on page 2, change "column 2 of Table" to column 2 of Table 1".

6) In Section 4 on page 5, delete the word relatively.

7) Table A.2 is messy, especially the HMAC and RNG.

8) In Section 9 on hash functions, the "*" in the chart should be an "a" in the row for SHA-1.

9) In Appendix A.3, I don't think the acronyms FFC, IFC, and ECC are defined anywhere in 800-131. Similarly, none of the math terms like order, subgroup, *MacLen*, or cofactor are not discussed in 800-131 as well.

From: Brian Weis [bew@cisco.com]

I am pleased to respond to the National Institute of Standards and Technology (NIST) with comments on the draft NIST Special Publication 800-131 dated January 2010. These comments are on behalf of the IETF Multicast Security Working Group, one of several groups in that body to develop Internet Standards Track documents.

DRAFT SP 800-131 describes an important and timely topic in cryptography today, namely the transitioning of cryptographic algorithms and key sizes to a higher level of strength. In general, it is clear in its recommendations of transitioning to stronger algorithms and consistent in its goal of transitioning to 112 bits of security strength. This is a valuable set of recommendations. However, we would like to call to your attention one exception that affects an Internet Standards Track document developed in the working group.

Table 7 of the DRAFT SP 800-131 indicates that the key wrapping method used by the GDOI protocol (RFC 3547) will no longer be allowed following December 31, 2010. The GDOI protocol was developed over the course of several years, first within the Secure Multicast Internet Research Group, and then within the IETF Multicast Security Working Group. Many individuals provided input during the development of the protocol, and it remains the only commercially available IETF Multicast Security Working Group key management method. There are no known Intellectual Property claims on this Internet Standard. We would like to suggest the following points for NIST to take into consideration, and possibly amend the recommendation in the DRAFT SP 800-131 document.

1. Security strength GDOI is a pair of exchanges that fit into the IKEv1 key establishment protocol, which remains an acceptable protocol within DRAFT SP 800-131. GDOI uses the same cryptographic methods and algorithms of IKEv1, and thus the security strength of the GDOI exchanges can be said equivalent to that of IKEv1. The GDOI protocol provides one additional cryptographic service, which is the distribution of secret keys from one participant to another participant. We appreciate that this service does require further consideration in your security strength analysis, and would like to take this opportunity to describe that service. Secret keys distributed in the GDOI protocol are not specially wrapped, but rather are wrapped with associated data by the strong confidentiality and integrity algorithms used by GDOI to protect its messages. In other words, we consider the protection of the keys and associated data to be a wrapping method. When strong cryptographic algorithms used by GDOI, 112 bits or more of security can be assured. The following discussion describes the key wrapping methods of each GDOI exchange.

The first is a registration exchange ("GROUPKEY-PULL") that protects the key agreement packets for confidentiality and integrity as described by IKEv1 (RFC 2409). Table 1 shows the cryptographic algorithms specified by Internet Standards that meet the recommendations of DRAFT SP 800-131.

Table 1. GROUPKEY-PULL

Use	Algorithms and Key Sizes	Security
Encryption	AES-128, AES-192, AES-	At least 128 bits

	256 (CBC mode)	
Hash Functions	SHA-1, SHA-256, SHA-384, SHA-512 (in HMAC mode)	At least 112 bits

The second is a rekey exchange ("GROUPKEY- PUSH") that protects the key agreement packets for confidentiality using a block cipher and integrity using a digital signature. Table 2 shows the cryptographic algorithms that can be used with the GROUPKEY-PUSH exchange that meet the recommendations of DRAFT SP 800-131.

Table 2. GROUPKEY-PUSH

Use	Algorithm and Key Sizes	Security
Encryption	AES-128, AES-192, AES-256 (CBC mode)	At least 128 bits
Digital Signature	DSA, RSA, ECDSA (all with key sizes meeting the recommendations)	With proper selection, at least 112 bits
Digital Signature Hash	SHA-256, SHA-384, SHA-512[11]	At least 112 bits

In summary, the strengths of cryptographic algorithms protecting secret keys and associated data all provide 112 bits of security or greater, which would seem to both meet the spirit and the letter of the requirements of DRAFT SP 800-131.

2. Testability

We understand that there is concern that the GDOI key wrap methods cannot be tested for their level of strength. As described in the previous section, the cryptographic algorithms are those that meet current NIST requirements, and the construction of those methods are well known. We would make the following comparison to the characteristics of the AES Key Wrap method. In the GDOI key wrap methods;

- Key Wrap is provided by a simple AES encryption in CBC mode. Appendix A.1 of DRAFT SP 800-131 clearly states that the smallest AES key size of 128 bits yields 128 bits of security.
- Key Unwrap is provided by a simple AES decryption in CBC mode.
- Key Data Integrity is provided in the GROUPKEY-PULL by an approved Hash function over the keys and associated data in HMAC mode as described in RFC 3547, where the definition of prf() can be found in RFC 2409.

[1] RFC 3547 does not explicitly refer to the SHA2 functions that provide a level of security great than 80 bits, however it is possible for implementations to use SHA2 functions with RFC 3547. Furthermore, a IETF Multicast Security Working Group document to explicitly add those definitions to the GDOI protocol is currently is in review (draft-ietf-msec-gdoi-update) and is expected to be published near the end of 2010.

- Key Data Integrity is provided in the GROUPKEY-PUSH by a digital signature, where the bytes of the message are signed using conventional digital signature algorithms and methods.

As shown, each of these operations can be evaluated for strength. The IETF Multicast Security Working Group would be pleased to provide a more detailed testability analysis upon request.

3. Transition time
DRAFT SP 800-131 recommends allowing a number of algorithms or bit sizes through 2010 only. In general, these recommendations have been well known and expected in the cryptographic community. However, the recommendation of only allowing GDOI through 2010 only does not have the same history. In fact, GDOI was only included as an approved method of key transport in FIPS 140-2 Implementation Guidance as recently as late 2009. The disallowance of GDOI a short time later is surprising.

It would be possible to update the GDOI Internet Standard to explicitly wrap secret keys and associated data with the informal specification for key wrapping currently allowed by NIST. Depending on the vagaries of the IETF standardization process, it may or may not be possible for standards actions to produce new protocol definitions meeting the recommendations in DRAFT SP 800-131 before the end of 2010. In any case, it is doubtful that both standards actions and product implementations could be completed in this timeframe. In the face of the draft recommendation disallowing GDOI altogether, it is highly improbable that a meaningful transition can occur for GDOI. We would request that if NIST must restrict the usage of the GDOI key wrapping methods that they allow current methods until 2013, which would provide for an orderly transition to a key wrap method explicitly approved by NIST.
In view of this analysis, we would ask NIST to reconsider its absolute restriction of GDOI after 2010,

We hope these comments are helpful to the NIST in developing the next version of the publication.

Please feel free to contact the Chair with any comments or questions.

Brian Weis
IETF Multicast Security Working Group Chair
bew@cisco.com
(408) 526-4796

From: Hintermeister Jan [Jan.Hintermeister@motorola.com]

1. On page 11, Section 9 on hash functions, the draft states that SHA-1 will be approved for use beyond 2010 in new and already validated implementations, for all applications except digital signature generation. This comment addresses the use of a digital signature for entity authentication as part of the Secure Shell (SSH) protocol.

   Section 8 of RFC 4253, "The Secure Shell (SSH) Transport Layer Protocol" describes Diffie-Hellman key exchange algorithm. As part of the key exchange, a digital signature is computed for the purposes of authentication. The key exchange methods described in the RFC require use of SHA-1 (section 8.2). If vendors are forced to use SHA-2 in implementations of SSH key exchange, the implementations will not be interoperable.

   The Diffie-Hellman key exchange described in section 8 using Group 14 will have the required key strength of 112 bits. The digital signature that provides entity authentication has 80 bits of strength. However, the digital signatures for SSH sessions will typically be short-lived.

   For the reasons above, I suggest that use of SHA-1 digital signatures for the SSH key exchange continue to be allowed past 2010.

2. On page 11, Section 9 on hash functions, the draft states that SHA-1 will be approved for use beyond 2010 in new and already validated implementations, for all applications except digital signature generation. Note (a) specifies that "non-digital signature applications" include "digital signature verification, HMACs, KDFs, RNGs and the approved integrity technique specified in Section 4.6.1 of FIPS 140-2."

   Note (a) does not mention "hash-only" in the list of applications for which SHA-1 is approved. I suggest that "hash-only" be added to the list in note (a). I think this would provide needed clarification, because Appendix A, section A-2 grouped digital signatures and hash-only applications in a single column.

   The fact that hash-only was specifically called out in A-2 but was not mentioned in Section 9 left this reader uncertain of NIST's intentions for SHA-1 in hash-only applications.

3. The draft document distinguishes between "new validations" and "already validated implementations". The final version of the document should carefully identify the criteria under which a module validation will be considered a "new validation" particularly with respect to revalidations. The existing draft document does not describe the circumstances under which a revalidation would be treated as a "new validation".

   .At a minimum, vendors should be allowed to make non-security relevant changes to an "already validated implementation" to maintain existing validations without triggering a "new validation" as described under scenario 1 in Implementation Guidance G.8. Vendors should have a way to maintain their existing products with bug fixes etc., while making the key strength changes required by NIST.

4. Scenario 3 in Implementation Guidance G.8 describes the situation where a vendor makes a security-relevant change. If making any security-relevant changes will cause the vendor's product to be considered a "new validation", then a vendor is essentially prevented from making incremental security upgrades, since any security upgrade will trigger a requirement to perform all the upgrades listed under "new implementation". This forces vendors to defer security upgrades until sufficient time and resources are available to make all the changes under "new implementation". Is that actually NIST's intent?

5. The FIPS 186-3 uses SHA-1 in several specific contexts. Will FIPS 186-3 be updated to require SHA-2 or will SHA-1 continue to be allowed for use for the applications defined in FIPS 186-3?

Jan Hintermeister
Motorola, Inc.
408-991-7532

From: Auston Holt [holt@atsec.com]

1. From a practical perspective, disallowing TLS 1.1 or TLS 1.0 in FIPS mode at the end of the year will create a serious disruption in Internet services because most browsers, end-user applications, and system services rely on the older versions and have not been upgraded to TLS 1.2. Disallowing TLS 1.2 will amount to a sheer crisis.

   Section 5.2, p.7 states:
   "Protocols are used for a very long time. When new versions of a protocol are designed and implemented, a module may need to include a capability to interoperate with both the new and existing protocols. Because of this, the KDFs in those existing protocols will continue to be allowed."

   Furthermore, Table 5 on p.8, in the next-to-last row states that KDFs in protocols listed in IG D.2 will be allowed for New Validations and Already Validated Implementations.

   However, IG D.2, p.112 states that a KDF may conform to the TLS KDF but only to December 31, 2010. At the same time, IG D.2, p. 113, states that the key transport scheme of TLS may be used in FIPS mode without a sunset date.

   This creates an apparent discrepancy that puts the fate of TLS in doubt. First, it does not make sense to allow the protocol for key transport, but disallow it for KDF - one cannot establish a channel over which to transport the keys. Second, disallowing the TLS KDF after December 31, 2010 is done without specifying which protocol versions will be eliminated. While there are legitimate concerns with TLS 1.0 and TLS 1.1 due to their reliance on SHA-1, TLS 1.2 is much better and independent of SHA-1. Third, in comparison, IG D.2 carefully distinguishes the versions of the IKE protocol and sunsets v1 at the end of 2010 but allows v2 indefinitely. The apparent discrimination of TLS with respect to IKE is not justified or substantiated by sound scientific arguments and thus appears arbitrary.

2. The column of "Bits of Security" specified in A.2 on page 13 was found to be confusing and misleading. For instance, according to the table in A.2, SHA-512 has the following bits of security: 80, 112, 128, 192 and 256.Actually, the security strength of SHA-512 is 256 bits. One may say that it has a security strength that is greater than or equal to 80/112/128/192/125 bits without running into inconsistency. Thus, it suggested to update the column of Bits of Security as the follows:

   "80" ---> ">=80"

"112" ---> ">=112"
"128" ---> ">=128"
"192" ---> ">=192"
"256" ---> ">=256"

The table in A.2 is taken from SP 800-57. NIST should make the same update in SP 800-57 as well.

Thank you very much,

Auston Holt
--
Auston Holt, atsec information security Deputy CST Lab Manager
mailto:holt@atsec.com - http://atsec.com - phone: +1-512-615-7392

From: James Knoke [JKnoke@cygnacom.com]

A. Section 1.2.2: The second sentence sort of contradicts section 1.2.3. Maybe just a little wordsmithing would help.

B. Section 1.2.4: "The date in the table refers to the date of the lab's submission of the test report to the validation authorities." could use some clarification. Are you talking about BOTH a plain algorithm submission to CAVP and a module submission to CMVP? I thought CMVP had not yet decided how to handle this timing. However, because of the long calendar time for CMVP to review submissions, it seems correct AND IMPORTANT for this wording about time of submission to apply to CMVP. Vendors and CSTs need to know the last date available for submission of modules containing "legacy" algorithms to CMVP because that date is under their control -- the date on which a module validation completes (or even goes into review) is not under their control.

C. Section 1.2.4: "The CMVP may take the appropriate actions" might benefit from a little wordsmithing. I think it would be *CAVP* that would modify an algorithm's validation certificate.

D. Section 1.2.4: "if a lab submitted a test report" -- same comments as above about whether CMVP has actually agreed to using the submission date of a module. Also what happens if a module is submitted in 2010, but does not complete validation until 2011 and some of the algorithms originally specified as allowed in FIPS mode are disallowed in 2011? Will the module validation be allowed to complete successfully, with no changes required to the implementation, but with the Security Policy (SP) and certificate being changed to simply have those "legacy" algorithms placed in the non-allowed? It is IMPORTANT for vendors to know how this will be handled and for CSTs to know how to advise their customers.

E. Section 1.2.4: If an algorithm becomes non-allowed in FIPS mode after 2010 in a validated module (or in a module which was submitted and otherwise heading for successful validation), will there be any requirement for the vendor to change the implementation or SP so that FIPS mode is properly documented or enforced (I think enforcement would be required in a level 3/4 module) to exclude use of the now-non-allowed algorithm? If so, the vendors will want to know since this could cause them a lot of grief. I think the intent is NOT to require these changes, but it might be worth making that crystal clear in the 800-131.

F. Section 2: You may want to make an explicit statement about whether decryption will be allowed after 2010 using the smaller key sizes.

G. Section 2: This is probably out-of-scope for 800-131, but you could add a statement about whether implementations of 3-key TDES must verify that all three input keys are different (especially in cases where TDES keys can be entered from an external source).

H. Section 5.2: In paragraph 2, "the KDFs in those existing protocols will continue to be allowed" should perhaps be clarified to specify KDFs allowed by IG D.2.

I. Section 5.2: In paragraph 3 there is mention of the cofactor, but table 5 does not mention the cofactor.

J. Table 6: For "Key Transport" the statements "Approved through 2010 only if the scheme is tested for compliance with SP 800-56B with $n = 1024$" seems ambiguous and to be redundant with "Any scheme with $1024 \leq n < 2048$ allowed through 2010 only". Perhaps the following wording would be more clear: "If the scheme is tested for compliance with SP 800-56B with $n = 1024$, it is approved through 2010 only".

K. Section 8: In the first paragraph, is it correct to say that a key derivation key could be obtained using a key wrapping algorithm?

L. Table 9: Typo for one of the superscripts.

M. Table 9: In the footnote, it would be good to clarify whether simple hashing is included as a non-digital signature application. Also SHA-1 may *not* be an "approved integrity technique" even now.

N. Section 10: Maybe this is out-of-scope for 800-131, but maybe it would make sense to state whether a module is disallowed from padding a short HMAC key up to 112 bits. FIPS 198-1 seems to allow such padding. SP 800-107 makes some statements along the lines of "An HMAC key shall be generated such that its security strength meets or exceeds the security strength required to protect the data over which the HMAC is computed", but does not explicitly address padding.

Jim Knoke
Lab Mgr and CC Evaluator, Security Evaluation Lab (SEL)
Lab Mgr, Cryptographic Equipment Assessment Lab (CEAL)
CygnaCom Solutions, Inc.
www.CygnaCom.com

JKnoke@CygnaCom.com
Tel: (703) 270-3578

Formatted: Bullets and Numbering

From: Tabram, Nicky [Nicky.Tabram@thales-esecurity.com]

1. Overview

Section 2 contains Thales e-Security's high-level view on the strategy presented by SP800-131 with respect to user uptake, business continuity and the practical aspects of undertaking the transition as currently planned. Specific comments on the publication itself is presented in Section 3. Please contact nicky.tabram@thales-esecurity.com for further correspondence regarding this document.

2. Commercial Considerations with Respect to User and Vendor Impact

2.1 Disruptive Impacts for Users and the Case for Gradual Transition

As the CMVP has become a global de-facto standard for cryptographic modules and HSMs with a reach far beyond the US federal government, many enterprise and government users of cryptography use products that have been certified to FIPS 140-2. In level 3, products are required to disable all non-approved algorithms and under the current proposals in SP800-131, 1024bit public key ciphers and SHA-1 will cease to be approved from 31st December 2010. This has the following consequences that may be unintended and will be disruptive to most current users of FIPS certified products, potentially either being counterproductive or leading to damage to the CMVP/FIPS brand.

1. There is a large global deployed estate of packaged software products (from PKI to SSL to application servers), and custom business applications that rely on the availability of 1024bit / SHA-1. Even many current software products fail to function without working implementations of these mechanisms. These applications often make use of cryptographic modules and HSMs via standard APIs and are deployed in conjunction with modules that are certified under the CMVP. The proposal to rescind NIST approval for these weaker algorithms will prevent vendors of cryptographic modules issuing maintenance updates if such updates are deemed "security relevant" and require full re-evaluation since the vendors would be required to deprecate weaker algorithms and thereby breaking compatibility with deployed products. This will deter vendors from issuing security patches or undertaking new FIPS evaluations after 2010, clearly both of these side effects are not consistent with the goals of SP800-131.

2. Products brought to market in 2011 will not be able to support SHA-1 or 1024-bit DSA, putting new products at a competitive disadvantage to products that are in the market prior to 2011. This may deter vendors from further investment and delay the availability of new technologies until the transition to 112bit effective security is complete. In particular this may prevent vendors investing in 112bit effective security where they are better able to serve non-federal markets by selling 80bit secure products that were certified prior to 2011.

3. Legacy ciphers will continue to be available where a product is used in a "non FIPS approved mode of operation". The proposed transition will force many users to

switch from FIPS approved to non-FIPS approved operation since SP800-131 and associated guidance effectively re-defines the functionality that is FIPS approved for certifications that start after 31st December 2010. Switching to a non-FIPS approved mode is likely to enable other legacy ciphers such as DES and MD5 and as such may serve to actually weaken security for customers who are forced into the temporary adoption of an unapproved mode of operation. Forcing customers to adopt a non-FIPS approved mode is counterproductive to the aims of SP800-131.

4. Awareness of SP800-131 is low among non-federal user groups. Users do not have budget set aside for upgrading applications and HSMs. The transition may cause users to defer upgrades to their HSM estates (leaving them with older and more vulnerable deployments), or it may lead to users deploying products that are approved to FIPS 140-2 level 2 or lower, including adoption of software-only cryptographic modules rather than HSMs. Both of these consequences will weaken security where SP800-131 is aiming to increase security.

Recommendations:

1. Vendors should be required to deliver secure products that offer 112bit effective ('internal') security after 2011. However customers should be free to use these secure products with applications that employ weaker algorithms - recognising that use cases and individual security policies vary. For example, 1024bit keys may remain perfectly acceptable when used throughout 2011 for SSL authentication but are clearly unsuited to personal credentials that are expected to have a 5-10 year life span. The CMVP should differentiate between a cryptographic module's internal strength of security and the range of algorithms it offers externally to users. The CMVP should mandate a minimum of 112bit effective security for cryptographic systems used to protect user keys but **should not** impose the new key size or hash algorithm restrictions on users at this time. Vendors are not well placed to force users to adopt stronger ciphers; and as mentioned above, Many users of FIPS cryptographic modules are not under federal mandate.

2. A well managed and effective transition requires some period of "parallel running" where users and vendors are able to support both new and old security standards while existing products and deployments are upgraded. The CMVP should explicitly allow full revalidation of existing products with the algorithms and key sizes that were applicable when the product was originally certified and without deprecating customer-facing 80bit functionality throughout 2011 and 2012. Without the ability to recertify old products under the original rules, there is no incentive or possibility for vendors to provide security patches to existing products or applications, as such patches would carry with them the disablement of algorithms in use.

3. For new products brought to market there could be a distinction for users between "pre SP800-131 FIPS mode" and "post SP800-131 FIPS mode". One approach would be for the FIPS approved mode of operation to transition from being a single binary flag to being a series of modes that could be numbered or dated. Hence

customers could choose to run in “legacy FIPS mode” or “new FIPS mode” as and when their applications are upgraded. Vendors should have the option to introduce such dual modes of operation in existing products; but implementing such a capability is likely to be a significant undertaking that cannot be completed before 2011.

4. Many systems rely on SHA-1 outside of digital signatures for authentication or integrity applications. The current stance of SP800-131 that allows SHA-1 to be used for non digital signature applications after 2010 is strongly supported.

2.2 Support for Continual of SHA-1 for Non-Signature Use

Many systems rely on SHA-1 outside of digital signatures for authentication or integrity applications. The current stance of SP800-131 that allows SHA-1 to be used for non digital signature applications after 2010 is strongly supported.

2.3 Timescales for Deprecating SHA-1 for All Uses

To assist in user and vendor planning SP800-131 should summarise timescales for deprecating SHA-1 for all uses and should re-confirm that 112-bit effective security is approved until 2030 (and is not likely, for instance, to come into scope of the 2015 review when RNG requirements are changed).

2.4 Potential User Confusion over FIPS 140-3 and SP800-131

Users are likely to be confused between FIPS 140-3 and the changes imposed by SP800-131. Consideration should be given to synchronising these changes.

2.5 Allowance of Sub-112-Bit Algorithms in Specific Applications

SHA-1 is still allowed to be implemented in cryptographic modules for non-signature uses, so an SP800-131 compliant module running in a FIPS 140-2 level 3 mode will contain an active implementation of SHA-1. Similarly, we understand from informal discussions with NIST that two-key TDES keys are allowed for payments applications but not for generic data encipherment so an SP800-131 compliant module running in a FIPS level 3 mode can also contain an active two-key TDES implementation. How will the CMVP assess compliance to level 3 when these algorithms are present? Will the module have to contain active code that restricts usage to an explicit ‘white list’ of higher-level applications, or an explicit black list, or nothing, or something else?

2.6 Expansion of CAVP

With many exceptions that are starting to appear (use of two-key TDES for payments applications being one of them), how will the CMVP/CAVP be expanded to include the additional, many and diverse algorithmic and usage considerations implied by this recommendation?”

3. Specific Comments on the Publication Itself

Section	Comment
General	The precedence of SP800-131 over SP800-57 should be clearly stated in the recommendation.
2	There is no supporting information on the security strength and approval status of GMAC, the integrity protection algorithm of GCM, under different authentication tag lengths (currently defined as 128, 120, 112, 104, or 96 bits as well as 64 and 32 bits in under certain restrictions)
3.1	SP800-131 mandates compliance with FIPS 186-3. With respect to RSA key generation this significantly changes the regime for primality testing that the CAVP/CMVP currently requires and will yield a significant performance degradation to end users. For some products RSA key generation is expected to be at least four times slower than when a product is operated in a FIPS approved mode of operation. When combined with a move to 2048bit key sizes, by way of a fair comparison an un-optimized software implementation may see 40x reduction is key generation performance, or approximately 250x reduction with 4096bit key sizes. Due to the significant performance impact of FIPS 186-3, and differing views of the merit of strong primality testing, implementation of the provable primality testing defined in FIPS 186-3 should remain a configuration option for users (against an alternative probable primality system to some known threshold) depending upon their security policy.
3.2	Through the reading of *Table 2: Digital Signature Security Strength Transitions* and *Appendix A.3 Recommended Algorithms and Minimum Key Sizes* that DSA using a key size of 1024 may continue to be used for the purposes of signature verification indefinitely (beyond 2010). It may be interpreted that beyond 2010 Certificates may continue to be generated in a non-FIPS approved manner using a 1024-bit key and subsequently verified in a FIPS approved manner. Given the spirit of the transition to move to minimum 112-bit security strength is this considered an acceptable practice? Clarification is required in this region. Note that this comment applies to Section 3 and footnote ‘a’ following Table 9.
5	Clarification required in Table 5 for the statement ‘Approved if the DH or MQV primitive is tested for compliance with SP800-56A’. I believe the intention of this is such that where a DH/MQV primitive is used with a non-approved KDF then this primitive generation may be tested. If this is the case, I feel it is important that it be stated that the primitive must be both compliant with SP800-56A ***and*** in accordance with Table 4 of SP800-131. Otherwise a loophole exists whereby it is possible to interpret that the DH

	primitive generation using an FA set is considered FIPS validated beyond 2010 simply by using a non-SP800-56A compliant KDF.
10	The draft states HMAC will continue to be approved beyond 2010 when a key of size 112 bits or more is used with any approved hash function. This imposes no requirements on the strength of the hash function. In particular this allows the continual use of HMAC-SHA1 which is according to Section A.2 to be of 128-bit strength. This is inconsistent with transition of digital signature algorithms (Section 3) where SHA-1 is considered to be of 80-bit strength, and its use for signature generation is being withdrawn. It is unclear why the difference in treatment of digital signatures and MACs as the collision attacks for the two types should be of the same order of complexity.
10	Some of our products have an HMAC validation for use with several flavours of SHA i.e. SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512, but there is no precise mention of key lengths. How is it ensured that NIST will not withdraw the HMAC certificate on our product that works with the keys 112 bits and more, when the supported key lengths have not been recorded?

From: Anthony Busciglio[abuscigl@cisco.com]

It is evident by the depth of detail in the publication that the NIST spent considerable time and study to develop this draft. When finalized, this standard will provide a roadmap for federal agencies to transition to a more secure state. Cisco supports this effort and will make its technical resources available to answer any questions the NIST may have.

Our full comments can be found below.

We hope these comments are helpful to the NIST in developing the cryptographic strength transition. Cisco firmly believes that considering industry input the transition to higher security strengths is essential for a smooth progression.

Please feel free to call or email with any comments or questions.

Regards,
Anthony Busciglio
Technical Marketing Engineer
Global Government Solutions Group
Cisco Systems, Inc.
abuscigl@cisco.com
(410) 309-5566

General Comments:

1. These recommendations show NIST's positive leadership in transitioning the industry to larger key sizes and away from uses of SHA-1 that are no longer appropriate. Though the recommendations do impose new requirements in these areas, there are strong technical motivations for these changes, the recommendations are pragmatic, and the direction of the changes were published years in advance, giving the industry time to prepare.

For example, the need to replace SHA-1 for use in digital signatures has been evident for years. The SHA-1 hash function has been shown to not meet the security goals for use in digital signatures, in a series of academic publications. SHA-2, the replacement for SHA-1, has been a FIPS for eight years, and the need to move to SHA-2 for signing has been articulated by NIST for three years. The recommendations also allow SHA-1 for uses other than digital signatures, which is both pragmatic and reflects the confidence that experts have in that usage.

Unfortunately, there are other requirements in this recommendation, especially the key derivation requirements implied by Table 5, and in the recent changes to the CMVP Implementation Guidance, that run counter to industry practice and which have no obvious technical underpinning. These proposed changes would make it impossible for vendors to simultaneously comply with NIST's cryptographic guidelines and with international standards, including the Secure Shell (SSH) protocol, Transport Layer Security (TLS) using Diffie-Hellman or Elliptic Curve

Diffie-Hellman, and the Internet Key Exchange version 1 (IKEv1). All of the named protocols are widely adopted and in use, including IKEv1. The U.S. Government has published Suite B profiles for TLS, SSH, and IKE; these proposed changes would force vendors to choose between supporting Suite B or the NIST guidelines. This is especially confusing considering that some Suite B documents specifically call out FIPS-140 conformance.

While the NIST guidance on key derivation appears to be technically sound, it excludes many other technically sound approaches, including ones developed by the IETF, IEEE, ISO, and ANSI. The excluded methods include some supported by detailed theoretical analyses and widely implemented in standards and products used by the U.S. Government. Please see the survey of key derivation functions recently published as http://tools.ietf.org/html/draft-irtfcfrg-kdf-uses-00.

These incompatibilities will hurt the industry and disrupt the U.S. Government agencies using cryptographic products. In principle, it would be possible to define alternative specifications for the TLS, SSH, and IKEv1 protocols. New versions of these protocols could be proposed, designed to conform to NIST guidelines. But standards development is a lengthy process typically measured on the scale of years, so this process could not take place by the 2011 deadline. It is not at all clear that the IETF would accept these new specifications as standards track. A vendor could unilaterally develop proprietary NIST-conformant variants of these protocols; this sort of proliferation of proprietary variants would create significant interoperability problems for the U.S. Government users of cryptography.

Some significant technical issues would arise in trying to reconcile SP-800-56a with IPSec, TLS, and SSH. The NIST specifications require different methods of key derivation, and require that identifiers for each participant in a protocol are included in the key derivation step. It is not at all clear what identifiers would be appropriate for these protocols. (For example, network addresses and ports can be dynamic, and a device can have multiple address or ports. Multiple devices can share a single address, as is used in load-balancing and NAT/PAT. Addresses and ports are frequently automatically translated as a packet traverses the network. Considering all of these factors, are addresses suitable for use as an identifier?

Would the key derivation need to be recomputed if the identifier changed?) The IETF protocols use a slightly different design paradigm, relying on a logical association between entities and nonces. It would be difficult to create a FIPS-140 version of these protocols without more clarity on these points.

Another obstacle to the creation of IKE or TLS protocol variants aimed at conforming to the proposed key derivation requirements is the fact that those protocols use their key derivation functions multiple times for multiple purposes (please see draft-irtf-cfrg-kdf-uses-00).

Within the NIST Cryptographic Toolkit, SP 800-56a and SP 800-108 specify distinct

functions for distinct purposes. While both IKE and TLS do provide some flexibility with regards to key derivation, it is impossible to design a single function that satisfies both specifications.

Even assuming that specifications were created for FIPS-140 variants of the TLS, IKE, and SSH protocols, it is not clear what could be gained by implementing them. Vendors and users have limited budgets for implementation, testing, and deployment; effort spent on developing variants of IETF standards that conform to SP 800-56a KDF would be effort taken away from other efforts like compliance with the other requirements in SP 800-131, Suite B and IKEv2.

Implementations would need to be larger, in order to support both the existing standards and the SP 800-56a KDF variants. Implementations would also be more complex, and would need a negotiation mechanism to determine which variant would be in effect. This complexity is likely to decrease the real-world assurance level provided by these implementations, while driving up their costs and the complexity of deploying and managing them.

NIST's CMVP Implementation Guidance has an exception in place for IKEv2 (but not the original version of the IKE protocol). It is encouraging that IKEv2 is allowed, but it is worrisome that it is allowed only as an exception, considering that other exceptions have recently been removed.

We ask that NIST reconsider its priorities, and review the technical suitability of the IETF protocols. If these protocols are sound, and we think they are, we suggest that NIST explicitly allow the use of these IETF standards for key derivation. Therefore, we are asking NIST to do two things: first, explicitly allow the use of these IETF protocols in a more permanent NIST document; and second, remove the proposed disallowance of the IETF protocols in this draft SP 800-131. We suggest that NIST engage with the IETF to develop specifications for how the IETF protocols can be implemented in a way that meets the security goals in the NIST Cryptographic Toolkit. If the review finds that the IETF protocols are unacceptable for technical reasons, we strongly encourage NIST to bring these reasons to the IETF and propose revisions to the standards. We expect that the entire industry will benefit from this standards cross-pollination. In any case we suggest revising the recommendations found in Table 5 of SP 800-131 to explicitly allow the use of IETF standards for key derivation.

2. How will revalidations of modules be handled? If previously validated modules that support 80-bit key strengths cannot be validated, government customers will be forced to use modules that are not up to date. Additionally, allowing the continued revalidation of modules will provide vendors the opportunity to validate versions of their products that support the more stringent key length requirements.

3. How will this transition address environments (presumably like many federal networks) that continue to support 80-bit strengths? Modules that enforce the new key

strength policies would effectively be in a position where they cannot communicate with a majority of the entities on the federal network.

Section Specific Comments

1. Last sentence in section 1.2.5, "For practical purposes, it may be necessary to extend the use of some algorithms, key sizes and protocols to allow a non-interruptive transition as agencies procure and replace legacy solutions," the meaning of this sentence is not clear.

   Does this imply transitions beyond what is described in the document? Please elaborate.
2. Section 3.1, FIPS 186-3 includes guidance revolving around assurance and use case for implementations of FIPS 186-3. Is the intention of SP 800-131 to require the additional assurances specified in FIPS 186-3 or to only require the cryptography specified in the standard?
3. Table 2, There are at least two classes of uses for Digital Signatures. The first usage class is to attest to the integrity and origin of long-lived information such as contracts, certificates and images. The second usage class is to provide a proof-of-possession of the private key associated with an assertion of identity.

   The first usage class exposes the signature for a long period of time (because of the type of data associated with the signature). Because of the long time exposure, it is critical to move as quickly as possible to utilizing the SHA-256 as the hashing algorithm in the generation of these signatures.

   The second usage class only exposes the signature to an attacker for a very short time (normally less than 1 second). They are used extensively in challenge/response exchanges with smartcards or other PK credential systems, and for certain types of protocols (e.g. SSL or TLS). Because the information is very ephemeral in nature and the signature is consumed/utilized within a very short time span, the opportunity for an adversary to create a colliding signature is extremely small. It would seem that allowing this type of signature to exist using SHA-1 for an additional period of time would not hurt the security of any of the current crypt-systems. While it is desirable to move to SHA-256 or higher in an expeditious manner, by granting an exception in this case, would allow the standards bodies like IETF and the implementers time for an orderly transition to utilizing the larger hash and will allow for extended time for the upgrade of existing crypto systems currently in use while maintaining a high degree of interoperability with these older systems.

4. Table 7, It appears that the intent of the document is to allow any approved cryptographic function for symmetric key wrapping. However, the document explicitly disallows GDOI after 2010 despite the fact that GDOI uses multiple approved cryptographic functions. GDOI is a group keying method which is beneficial to users because it allows protection of multicast traffic. The only practical method of protecting multicast traffic is through the use of group keys with a group keying method, and GDOI is the accepted industry standard. The document

appears to actually ban the use of GDOI after 2010 which would be quite problematic. If the intent is to allow GDOI only if it uses approved cryptographic functions, that is the right approach and the document should simply state that. Please note that GDOI can use a variety of key sizes including AES-128, AES-192, and AES-256. The NIST Cryptographic Toolkit currently does not provide for group key management. The NIST Cryptographic Toolkit, and NIST SP 800-131, should therefore allow for, and support, the use of group keying methodologies. GDOI is an international standard, well accepted, and secure methodology for providing group keying, and therefore should be explicitly allowed.

Disallowing GDOI in FIPS mode will be a great disservice to industry and federal governments around the world. GDOI is widely used throughout the financial, insurance, and federal markets to ensure traffic is protected over MPLS networks. Each of these industries requires FIPS 140 validated modules as a procurement criterion. Worldwide there are over 400 institutions deploying GDOI in their protected network with a combined total of 10,000 group members. It is anticipated that the number of group members in protected networks using GDOI will grow to 15,000+ within the next year.

GDOI provides a service that the allowed key wrap mechanisms were not designed to provide. When compared to AES and TDES key wrap, GDOI provides the same level of confidentiality and integrity at an order of magnitude more quickly amongst multiple communicating parties. Disallowing GDOI in FIPS mode will reduce the security/usability of MPLS networks by forcing parties on the network to either send traffic unencrypted or use a significantly less efficient AES or TDES key wrap solution.

5. Section 7: We believe that the intent of SP 800-131 and the current Implementation Guidance is that AES or Triple DES can be used in any NIST-approved modes to provide the key wrapping service, and we believe that this permissive policy is suitable because of the lack of any accepted standard for key wrapping. We suggest that the intent be clarified with an explicit statement.

We also encourage NIST to further refine its definition of the key wrapping service and the requirements around its usage, and to emphasize the distinction between the abstract idea of the service and the draft 2001 algorithm with the same name. Alternatively, it may be more useful to construct requirements for symmetric key transport.

We discourage any preferment of the draft 2001 Key Wrap algorithm because of its technical deficiencies. It provides only weak integrity protection, it does not allow for associated authenticated but unencrypted data, it has alignment restrictions, and its computational cost is several times higher than other block cipher modes of operation. There are block cipher modes of operation that do not have these limitations – XCB, EME2, and SIV, for instance.

In addition, the key wrapping or key transport service can already be provided by using appropriate components from the NIST Cryptographic Toolkit.

6. Section 8: For protocols in which both SP 800-56a and SP 800-108 may be applicable, what is the delineator for when SP 800-56a should be followed and when SP 800-108 should be followed?

7. Section 10: GMAC is omitted. Is this intentional? It is expected that it is omitted because there is no transition issues associated with it. It might be easiest to just add the sentence "There are no transition issues for SP 800 38 D" for clarification.

8. Table 10, Our interpretation is that HMAC-SHA-1 is allowed beyond 2010, because both its key size and its security level (as described in A.2) exceed 112 bits. We suggest that this point be clarified by including an explicit statement. Considering that HMAC-SHA-1 provides an adequate security level and its use is prevalent, we strongly agree with the decision to continue allowing its use.

From: Vijay Bharadwaj [Vijay.Bharadwaj@microsoft.com]

Thank you for the opportunity to review this document, and for all the work you have done in expanding and clarifying this document since the previous draft. We agree with the goals of this transition and believe that it will have a positive effect on security overall. However, we have a few concerns about the details of this document, especially with regard to compatibility:

1. Section 3.2 states that digital signatures with security strengths less than 112 bits will be disallowed after 2010. However, SP 800-57 Part 3 (published December 2009) recommends (in Section 8.1.4) use of 1024-bit RSA keys with SHA-1 to sign DNSSEC zone records until 2015. It is unclear how this interacts with the SP 800-131 transition. Will NIST be making an exception for DNSSEC (and other protocols using short-lived 1024-bit RSA signatures) until 2015, or is it NIST's intention to modify the SP 800-57 Part 3 guidance with this document? Similar concerns apply to use of SHA-1 in NSEC3.
2. Section 6 states that any schemes not tested for compliance with SP 800-56B will not be allowed after 2013. However, many widely deployed protocols use RSA-based key transport schemes other than the ones found in SP 800-56B. For instance, TLS 1.2 uses RSA in PKCS#1v1.5 padding mode, and it seems unlikely that the installed base of TLS will move over to an SP 800-56B scheme by 2013. We believe that a more gradual transition plan should be followed here, with IG guidance to allow for existing schemes to continue until new and revised protocols (containing SP 800-56B compliant schemes) are ubiquitous, and primitives-level testing for RSA if desired.

Thanks,

--
Vijay Bharadwaj
Microsoft Corporation

From: Santosh Chokhani [SChokhani@cygnacom.com]

I want to thank you for putting together a comprehensive document that identifies and pulls together in one place all the recommendations and requirements that have been promulgated in the past.

Addressing the following issues will further enhance the guidance to the vendors and to Federal Agencies.

1. The document should identify the circumstance under which FIPS rating of a module will be invalidated. This should be tied to a time line so that the Federal agencies can plan for replacement cryptographic modules.

2. Transition to SHA-256 should take risk management based approach since it does not appear that application usage of SHA-256 will be available for digital signature in the most commonly installed based of clients: Windows XP with SP3. The risk management approach should consider which classes of objects have practical hash collision threat. Those classes of objects with exploitable hash collision should be required to SHA-256. It is possible that this would be largely public key certificates which Windows XP with SP3 processes.

3. The Draft SP 800-131 should clarify if hashing in support of digital signature for authentication purposes in SSL/TLS protocol requires SHA-256, e.g., in client authenticated TLS when client is using RSA algorithm for authentication. It would seem that while the certificates in the certification path should be signed using SHA-256 hash, the actual protocol data can be hashed and signed using SHA-1 since collision threat does not materialize due to random data contributed by both parties and real-time nature of the protocol.

4. The Draft SP appears to prohibit PKCS 1, version 1.5 for key transfer beyond 2013. The following impacts should be considered of this decision and timeline:
   a) This may have significant impact on interoperability with non US Federal partners.
   b) What activities need to be undertaken with IETF and other standards bodies to standardize algorithm OIDs and cipher suites, and potential signaling mechanisms so that producers and consumers of the payload for the various protocols (e.g., TLS, S/MIME) know the algorithm to use.
   c) If algorithm OIDs need to change in the public key certificates (e.g., subject public key information), consider the de facto standard of 3 year certificates to determine the achievable transition dates. These may be 2013 or later.

5. The draft SP is silent on requirement for key generation for RSA in accordance with FIPS 186-3. Based on informal survey of the industry, this is another area that requires some lead time.

6. The draft SP is silent on at what point it would be desirable for relying party systems to have technical means to reject 80 bit security algorithms. Note that the commercial products do not easily support this feature.

Santosh Chokhani
CygnaCom Solutions

From: Chris Brych [cbrych@nuvo.com]

There are a few points I wanted to bring to your attention. The first is regarding the algorithm transition plan regarding use of signatures. As part of performing an ephemeral Diffie-Hellman key agreement function, a sign operation is required that makes use of a modulus size of 1024 with SHA-1. Will this operation be allowed or not allowed as part of the rules governing use of signature generation operations using 1024 bit modulus sizes and SHA-1?

Regards,

Chris

Chris Brych
Director, DOMUS IT Security Laboratory
400 March Road, Suite 190
Kanata, Ontario
K2L 1A1
Canada
Email: cbrych@domusitsl.com
web: www.domusitsl.com
Office: 613-726-5091
Cell: 613-867-1241
Fax: 613-248-4948

From: Joan Lozano [jlozano@infogard.com]

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
1		General comment for the draft.	The references to "Recommendation" should be changed to "document".	Once SP 800-131 is finalized and no longer a draft, the references to "Recommendation" should be removed from the document.
2	Page 2, last paragraph	If the tables proposed by InfoGard (included in our submission package) are acceptable, then the last paragraph on page 2 is not necessary.	Remove the last paragraph on page 2.	The tables (included as part of InfoGard's comment submission) separating what is Approved and what is undergoing transition should be clearer and reduces the number of scenario examples that need to be clarified in the document.
3	Section 1.2.4	There should be a distinction between algorithm validations and cryptographic module validations. Combining the two topics in Section 1.2.4 is confusing.	**Section 1.2.4 – New Validations and Already Validated Algorithm Implementations and Cryptographic Modules** This document contains several tables addressing algorithm implementations and cryptographic modules. - *New Validations* are the cryptographic modules that are being tested by an accredited CST laboratory	The guidance for cryptographic modules should come from an Implementation Guidance and not in this document. The CMVP should reference the SP 800-131 document as a point of reference.

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
			for which the test report has been submitted to CMVP under FIPS 140-2 Implementation Guidance G.8, Scenarios 3 and 5. For algorithm implementations, *New Validations* are the algorithm implementations that are being tested by an accredited CST laboratory for which the algorithm results have been submitted to the CAVP. The date in the table refers to the date of the CST lab's submission of the module test report or algorithm results to the validation authorities. *Already Validated* cryptographic modules and algorithm implementations have been validated and issued certificates by the CMVP or CAVP. The CMVP and CAVP will review these modules and the underlying algorithm implementations for the purpose of their compliance with the new security requirements as stated in this document. … Suggest removing: The CMVP may take the appropriate actions, which	

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
			may include the modification or the revocation of the module's or algorithm's validation certificate. Due to the complexity of the available information at the module level, the CMVP actions are as yet undecided.	
4	Section 3.1, 5th paragraph	Terms used in this document should be consistent. The reference to "currently-validated" should be "already validated".	Note that the invalidation of the algorithm certificates will affect all already validated FIPS 186-2 DSA implementations, as well as those implementations of RSA and ECDSA that only use SHA-1 for digital signature generation.	Terms used in this document should be consistent.
5	Section 4, Table 3	In Table 3 (RNG Transitions), ANSI X9.62-2005 (HMAC) is listed as an Approved RNG (now and beyond 2010). This algorithm is currently not listed in FIPS 140-2 Annex C.	Remove the ANSI X9.62-2005 RNG reference from Table 3.	Including the ANSI X9.62-2005 RNG in Table 3 is confusing because it is not in Annex C. If the ANSI X9.62-2005 RNG is truly equivalent to one of the SP 800-90 RNGs, then listing the SP 800-90 RNGs is sufficient.
6	Section 5	IG D.2 is contradictory in some ways to SP 800-131 Section 5.	Remove IG D.2 entirely and fold it into SP 800-131.	The information contained in IG D.2 is more appropriate in SP 800-131. The maintenance of one document would be more

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
				manageable as well as reducing inconsistencies.
7	Section 5.2, 3rd sentence, Table 5, Footnote in Table 5, Section 6, Section 7	Unnecessary references if IG D.2 is removed.	In many cases, the use of the combination of the primitive and KDF used in a protocol has been deemed as "allowed" and included in a list of such protocols in Appendices A4 and A5 of this document.	Consistency.
8	Section 9, Table 9	In Table 9 (Hash Function Transitions), it states that SHA-1 is "Approved for digital signatures generation through 2010 only". This statement should be clarified to include hash-only usage, which is also affected by the 2010 transition according to SP 800-57.	In Table 9 (row 1, columns 2 and 3), change the following from: "Approved for digital signatures generation through 2010 only" to "Approved for hash-only and digital signatures generation through 2010 only"	This modification will be consistent with SP 800-57 Table 3 (and Appendix A.2 of SP 800-131).

ENCRYPTION ALGORITHM TABLES

Table 1a: Approved Encryption Algorithms

Encryption Algorithm	New Validations	Already Validated
Three Key Triple-DES	OK	OK
AES 128	OK	OK
AES 192	OK	OK
AES 256	OK	OK

Table 1b: Transition for Encryption Algorithm

Encryption Algorithm	New Validations	Already Validated
Two Key Triple-DES	Approved through 2010 only	Approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"
Skipjack	Approved through 2010 only	Approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"

Note: CST labs may submit algorithm results to the CAVP through December 31, 2010.

DIGITAL SIGNATURES STRENGTHS TABLES

Table 2a: Approved Digital Signatures Strengths

Digital Signature Process	New Validations	Already Validated
Signature Generation	OK for ≥112 bits of security	OK for ≥112 bits of security
Signature Verification	OK	OK

Table 2b: Transition for Digital Signatures Security Strengths

Digital Signature Process	New Validations	Already Validated
Signature Generation	≥80 bits and <112 bits of security approved through 2010	≥80 bits and <112 bits of security approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"

Note: CST labs may submit algorithm results to the CAVP through December 31, 2010.

RANDOM NUMBER GENERATION TABLES

Table 3a: Approved Random Number Generation

Description	New Validations	Already Validated
RNGs specified in SP 800-90 (HASH, HMAC, CTR, DUAL_EC) and ANS X9.62-2005 (HMAC)	OK	OK

Table 3b: Transition for Random Number Generation

Description	New Validations	Already Validated
RNGs specified in FIPS 186-2, ANS X9.31-1998 and ANS X9.62-1998	Approved through 2010 only	Approved through 2015 only[a] with caveat "transitional phase only – valid until December 31, 2015"

Note: For new validations, CST labs may submit algorithm results to the CAVP through December 31, 2010. Already validated RNG implementations specified in Table 3b are approved for use through 2015. A cryptographic module implementing these RNGs undergoing a revalidation (IG G.8 #3) shall go through a transitional phase ending in 2015.

[a] While some uses of Two Key Triple DES will no longer be approved after 2010 (e.g., see Section 2), implementations of the RNG in ANS X9.31 that use Two Key Triple DES will continue to be approved through 2015.

SP 800-56A KEY AGREEMENT (DH AND MQV) TABLES

Table 4a: Approved SP 800-56A Key Agreement (DH and MQV)

Scheme	New Validations	Already Validated
SP 800-56A primitives and KDFs using finite fields	OK for Parameter sets FB and FC	OK for Parameter sets FB and FC
SP 800-56A primitives and KDFs using elliptic curves	OK for Parameter sets EB-EE	OK for Parameter sets EB-EE

Table 4b: Transition for SP 800-56A Key Agreement (DH and MQV)

Scheme	New Validations	Already Validated
SP 800-56A primitives and KDFs using finite fields	Parameter set FA approved through 2010 only	Parameter set FA approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"
SP 800-56A primitives and KDFs using elliptic curves	Parameter set EA approved through 2010 only	Parameter set EA approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"

Note: CST labs may submit algorithm results to the CAVP through December 31, 2010.

KEY AGREEMENT (DH AND MQV) FOR MODULE IMPLEMENTATIONS NOT FULLY COMPLIANT WITH SP 800-56A TABLES

Table 5a: Approved/Allowed Key Agreement (DH and MQV) for Module Implementations Not Fully Compliant with SP 800-56A

Scheme	New Validations	Already Validated
DH and MQV primitives using finite fields	OK if the DH or MQV primitive is tested for compliance with SP 800-56A with $\|p\| \geq 2048$ bits and $\|q\| \geq 224$ bits	OK if the DH or MQV primitive is tested for compliance with SP 800-56A with $\|p\| \geq 2048$ bits and $\|q\| \geq 224$ bits
DH and MQV primitives using elliptic curves	OK if the DH or MQV primitive is tested for compliance with SP 800-	OK if the DH or MQV primitive is tested for compliance with SP 800-

	56A with $\|n\| \geq 224$ bits	56A with $\|n\| \geq 224$ bits
KDFs in protocols listed in IG D.2	OK	OK

Table 5b: Transition for Key Agreement (DH and MQV) for Module Implementations Not Fully Compliant with SP 800-56A

Scheme	New Validations	Already Validated
DH and MQV primitives using finite fields	Any[b] DH or MQV implementation with $1024 \leq \|p\| < 2048$ bits, and $160 \leq \|q\| < 224$ bits allowed[c] through 2010 only Any[b] untested DH or MQV implementation with $\|p\| \geq 2048$ bits, and $\|q\| \geq 224$ bits allowed[c] through 2013 only	Any[b] DH or MQV implementation with $1024 \leq \|p\| < 2048$ bits, and $160 \leq \|q\| < 224$ bits allowed[c] through 2010 only with caveat "transitional phase only – valid until December 31, 2012" Any[b] untested DH or MQV implementation with $\|p\| \geq 2048$ bits, and $\|q\| \geq 224$ bits allowed[c] through 2013 only with caveat "transitional phase only – valid until December 31, 2013"
DH and MQV primitives using elliptic curves	Any[b] DH or MQV implementation with the $160 \leq \|n\| \leq 223$ bits allowed[c] through 2010 only Any[b] untested DH or MQV implementation with $\|n\| \geq 224$ bits allowed[c] through 2013 only	Any[b] DH or MQV implementation with the $160 \leq \|n\| \leq 223$ bits allowed[c] through 2010 only with caveat "transitional phase only – valid until December 31, 2012" Any[b] untested DH or MQV implementation with $\|n\| \geq 224$ bits allowed[c] through 2013 only with caveat "transitional phase only – valid until December 31, 2013"
KDFs not in SP 800-56A nor explicitly listed in IG D.2	Allowed through 2010 only	Allowed through 2010 only with caveat "transitional phase only – valid until December 31, 2012"

a $|p|$, $|q|$ and $|n|$ are used to denote the bit length of p, q and n, respectively.

b The DH or MQV primitives may or may not be specified in SP 800-56A.
c The DH or MQV primitive is allowed without testing or vendor affirmation of compliance with SP 800-56A in accordance with IG D.2.

RSA-based KEY AGREEMENT AND KEY TRANSPORT KEY SIZES TABLES

Table 6a: Approved RSA-based Key Agreement and Key Transport Key Size

Scheme	New Validations	Already Validated
Key Agreement[a]	OK for n = 2048	OK for n = 2048
Key Transport[b]	OK if the scheme is tested for compliance with SP 800-56B with n = 2048	OK if the scheme is tested for compliance with SP 800-56B with n = 2048

Table 6b: Transition for RSA-based Key Agreement and Key Transport Key Size

Scheme	New Validations	Already Validated
Key Agreement	n = 1024 bits Approved through 2010 only	n = 1024 bits Approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"
Key Transport	Any[c] scheme with $1024 \leq n < 2048$ allowed through 2010 only Approved through 2010 only if the scheme is tested for compliance with SP800-56B with n = 1024 Any[c] untested scheme with $n \geq 2048$ allowed through 2013 only	Any[c] scheme with $1024 \leq n < 2048$ allowed through 2010 only with caveat "transitional phase only – valid until December 31, 2012" Approved through 2010 only if the scheme is tested for compliance with SP800-56B with n = 1024 with caveat "transitional phase only – valid until December 31, 2012" Any[c] untested scheme with $n \geq 2048$ allowed through 2013 only with caveat

[a] Key agreement using RSA is only specified in SP 800-56B, where n is specified as either 1024 or 2048 bits in length
[b] RSA key transport schemes existed prior to the development of SP 800-56B, and therefore, need to be accommodated during a transition period.
[c] The RSA key transport schemes may or may not be specified in SP 800-56B.

		"transitional phase only – valid until December 31, 2013"

KEY WRAPPING KEY SIZES TABLES

Table 7a: Allowed Symmetric Key Wrapping Key Size

Algorithm	New Validations	Already Validated
AES	OK	OK
Three-Key Triple-DES	OK	OK

Table 7b: Transition for Allowed Symmetric Key Wrapping Key Size

Algorithm	New Validations	Already Validated
Two Key Triple DES	Allowed through 2010 only	Allowed through 2010 only with caveat "transitional phase only – valid until December 31, 2012"
GDOI protocol (described in IETF RFC 3547)[a]	Allowed through 2010 only	Allowed through 2010 only with caveat "transitional phase only – valid until December 31, 2012"

KEY DERIVATION FUNCTION TABLES

Table 8a: Approved Key Size Transitions for a Key Derivation Function

Algorithm	New Validations	Already Validated
HMAC based KDF	OK	OK
CMAC based KDF	OK for AES and Three Key Triple DES-based KDFs	OK for AES and Three Key Triple DES-based KDFs

Table 8b: Transition for Key Size Transitions for a Key Derivation Function

Algorithm	New Validations	Already Validated
CMAC based KDF	Two Key TDES-based KDF Approved through 2010 only	Two Key TDES-based KDF Approved through 2010 only with caveat

[a] The GDOI protocol is listed as an allowed protocol in Appendix xx of this document.

		"transitional phase only – valid until December 31, 2012"

HASH FUNCTIONS TABLES

Table 9a: Approved Hash Functions

Hash Function	New Validations	Already Validated
SHA-1	OK for all non-digital signature generation applications	OK for all non-digital signature generation applications
SHA-224, SHA-256, SHA-384, and SHA-512	OK	OK

Table 9b: Transition for Hash Functions

Hash Function	New Validations	Already Validated
SHA-1	Approved for digital signatures generation through 2010 only	Approved for digital signatures generation through 2010 only[a] with caveat "transitional phase only – valid until December 31, 2012"

MESSAGE AUTHENTICATION CODE TABLES

Table 10a: Approved Message Authentication Code

MAC Algorithm	New Validations	Already Validated
HMAC	OK for Key lengths ≥ 112 bits	OK for Key lengths ≥ 112 bits
CMAC	OK for AES and Three Key Triple DES	OK for AES and Three Key Triple DES

Table 10b: Transition for Message Authentication Code

MAC Algorithm	New Validations	Already Validated

[a] Includes digital signature verification, HMACs, KDFs, RNGs, and the Approved integrity technique specified in Section 4.6.1 of FIPS 140-2.

HMAC	Key lengths ≥ 80 bits and < 112 bits Approved through 2010 only	Key lengths ≥ 80 bits and < 112 bits Approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"
CMAC	Two Key Triple DES Approved through 2010 only	Two Key Triple DES Approved through 2010 only with caveat "transitional phase only – valid until December 31, 2012"

From: Andras Szakal [aszakal@us.ibm.com]

More input from our systems teams.

TPM Comment: In appears that under this NIST draft:
- TPM-original is only valid thru this years. Is that true?
- There does not appear to be alignment between NIST's view of SHA-1 and TCGs ability to specify the TPM-next. (SHA-2 or more).

Crypto Algorithm	System SSL FIPS Mode Today	Transition Document	Work Effort Required	Comments/Questions
Symmetric Algorithms	3-key TDES, AES 128, 256	3-key TDES, AES 128, 256	None	
Digital Signature Generation	RSA – PKCS #1.5 – key sizes 1024-4096 DSA – key sizes 1024 only	1024-2048 through 12/31/2010 2048 and greater beyond 2010	Restrict keys < 2048 What do we do about DSA? We do not support 2048?	There has been some discussion that RSA 4096 is not allowed in FIPS mode. Currently SSL supports this. For R11, we are going to state in Security Policy that 4096 is not supported in FIPS mode and it is the responsibility of the application to control usage. Do we really need to restrict 4096 RSA?
Digital Signature Verification	RSA – PKCS #1.5 – key sizes 1024-4096 DSA – key size1024 only	1024 and greater allowed	None May need to add DSA 2048 support if added for generation requirement	There has been discussion that RSA 4096 is not allowed in FIPS mode. Currently System SSL supports this. For R11, we are going to state in Security Policy that 4096 is not supported in FIPS mode and it is the responsibility of the application to

				control usage. Do we really need to restrict 4096 RSA?
Random Number Generation	FIPS 186-2, ANSI X9.31	New validations: FIPS 186-2 and ANSI X9.31 through 2010 Already-validated: FIPS 186-2 and X9.31 through 2015 Replace version SP 800-90 or ANSI X9.62-2005 can be used now	Currently, we meet the FIPS 186-2 and X9.31 criteria. Since good until 2015 – first release needing new level is R14 that will GA in 2012.	Spoke with Tamas – he has a version of RNG that meets the new requirement. Could retrofit into SSL RNG. Need to confirm SHA-1 usage OK. Footnote in Section 9 implies it is OK.
Diffie-Hellman	2048-bit key size only – not sure about subgroup bit size	2048 or greater with subgroup bit length of 224. Untested DH must pass test compliance by 12/31/2013	Need to investigate implementation (which standard, bit sizes, etc.) Need to have implementation compliance tested for R15.	Do not know which standard implementation maps to? PKCS #11 tokens currently support subgroup bit length of 160. What do we do about prior evaluations that are no longer valid?
RSA Key Generation	1024-4096 key sizes ANSI X9.31-1998			Not sure if there are any strict requirements. Investigation is needed. Confirm RSA key generation not impacted.
RSA Key Transport (Wrapping)	TLS V1.0, TLS V1.1 – RSA key sizes 1024-4096	Allowed – ANy scheme using 1024-2048 through 2010	Need to determine if implementation is compliant with SP 800-	There is a note about needing to be accommodating to existing transport schemes during the

		Allowed – Any untested scheme using ≥ 2048 through 2013. Approved if tested for compliance with SP 800-56B and key size 2048	56B and what type of testing is needed.	transition period. Not sure what that means. Does that mean TLS V1.0 and TLS V1.1 will be allowed.?
Hash Functions	SHA-1 and SHA-2	SHA-1 allowed for digital signature generation through 2010. SHA-1 approved for all non-digital signature applications. SHA-2 approved for hash functions		Does this mean that we can use SHA-1 for the TLS handshake (no client auth/no DH) messages, RNG (Footnote in Section 9 implies it is OK) and hashing of our key database files? Looks like SHA-1 based HMACs are allowed. We will need to restrict certificate usage to RSA certs signed with SHA-2 when dealing with certificates.
RSA Encrypt/Decrypt				Do not see any mention about this. Has this changed? Assume it has the same restrictions as digital signatures.

From: Joan Lozano [jlozano@infogard.com]

Here is another document that we'd like to submit as supporting documentation to our SP 800-131 comments.

Recommended 2 Year Transition Plan - Algorithms with <112 Bits of Security

Please note that the DES Transition Plan was used to draft this recommendation. It is recommended that this notice be distributed in conjunction with SP 800-131.

Background: We recommend that transitions be handled similarly to the DES Transition (as described in the DES Transition Plan document, http://csrc.nist.gov/groups/STM/common_documents/DESTranPlan.pdf). This document can then be used to point to SP 800-131 as the reference document.

Rationale: We recommend a 2-year transition period starting January 1, 2011 for current FIPS modules and Revalidations containing algorithms with <112 bits of security. A two year transition period will provide time for industry and the Federal Government to respond to the new requirement. Following are key issues that necessitate an appropriate transition period:

Interoperability Impact: Many (if not most) current protocol implementations contain algorithms with <112 bits of security (e.g., implementations of key exchange in TLS, SSH, and IKE protocols). In some cases, protocols do not have the full capability for 112 bits yet (e.g., SSH key exchange authentication performs signature generation with SHA-1 only, RFC 4253 Section 6.6). Even if Vendors could respond with new designs implementing protocols utilizing algorithms with ≥112 bits of security, they would be incompatible with the enormous infrastructure in place within the government agencies. Upgrading protocol standards and module implementations for proper interoperability will entail time and effort. A 2-year transition period, though aggressive, will allow time to plan and implement proper interoperability between FIPS modules and other existing modules.

Schedule Impact: Planning, developing, testing, validating, researching, approving, and purchasing FIPS validated modules takes time, especially within the Department of Defense which is the largest consumer of validated cryptographic modules. CST Laboratories must test these algorithms and modules. Federal Agencies must plan, procure, and implement upgrades to their existing infrastructure to support algorithms with ≥112 bits of security to support the purchase of new products that met the ≥112 bit security requirements.

Cost Impact: The cost for Federal Agencies and the Department of Defense, in particular, of upgrading existing infrastructure for interoperability and new procurements to meet the required ≥112 bits of security will be significant. The appropriation and allocation of funds will take time and put stress on the budget.

The purpose of this transition period is to allow for the upgrade and revalidation of existing cryptographic modules. New modules will be required to implement algorithms with ≥112 bits of security.

Recommended Transition Plan *(content similar to the DES Transition Plan)*:

The Cryptographic Module Validation Program (CMVP) Algorithm and Key Size Transition Plan addresses the use of algorithms with <112 bits of security by Federal Agencies, which are incorporated in cryptographic modules, validated to FIPS 140-1 or FIPS 140-2. This transition plan was developed to allow Federal Agencies and vendors to smoothly transition to stronger Approved security functions. Please reference SP 800-131 which addresses the use of algorithms and key sizes.

1. Effective January 1, 2011: Federal Agencies may continue to use algorithms with <112 bits of security as NIST recommended Approved security functions in a FIPS Approved mode of operation in FIPS 140-1 or FIPS 140-2 validated cryptographic modules for a period of 2 years (until December 31, 2012). This provides a transition period to migrate to stronger Approved security functions.

    a. Cryptographic modules validated to FIPS 140-1 or FIPS 140-2 that implement an algorithm with <112 bits of security as an Approved security function will have the algorithm entry on the module validation list changed to include the caveat "transitional phase only – valid until December 31, 2012".

    b. The Cryptographic Algorithm Validation Program (CAVP) will discontinue the issuance of new algorithm validation certificates with <112 bits of security as of January 1, 2011 (Note: Algorithm implementations under contract for testing by a CST Laboratory prior to December 31, 2010 will be completed).

    c. Agencies must understand that NIST strongly recommends against any continued use of algorithms with <112 bits of security. Agencies must accept the security risks of the continued use of algorithms with <112 bits of security during the transition phase. In short, algorithms with <112 bits of security do not provide adequate protection for data whose confidentiality must be assured for more than near-transitory implementations.

2. After the 2-year transition period ends on December 31, 2012:

    a. Algorithms with <112 bits of security will be removed from FIPS 140-2 Annex A, *Approved Security Functions*.

    b. The CMVP will move all references of algorithms with <112 bits of security from an Approved security function to the non-Approved security function line on all FIPS 140-1 and FIPS 140-2 cryptographic module validation certificates. Modules validated to FIPS 140-1 or FIPS 140-2 that *only* implement algorithms

with <112 bits of security as Approved security functions will have their entry on the module validation list annotated as not meeting FIPS 140-1 or FIPS 140-2 requirements anymore and can no longer be used by a Federal agency.

c. The CAVP Validation List for the algorithms identified above will be saved for historical reference only, but annotated as no longer being Approved for use.

From: Shu, Jonathan [jonathan.shu@osd.pentagon.mil]

The Department of Defense's Comments on NIST SP 800-131 – as of March 18, 2010

Legend (type of comment)

E = Editorial
G = General
T = Technical

ID	ORG	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1	DoD	DoD PKI PMO	N/A	G	The Department of Defense has already formally responded to NIST's request for comments regarding Draft SP 800-131 via a memo from DoD Deputy Chief Information Officer, David M. Wennergren, dated March 12, 2010. The DoD offers these detailed comments in support of that memo. Draft SP 800-131 greatly expands the scope of standards which are subject to a December 31, 2010 timeline versus what was required under previously published SP's. Whereas previous NIST SP's applied the 12/31/10 timeline to a limited scope of functions for specific purposes (i.e. hash functions and digital signatures on PIV Objects, End Entity Certificates, CRL's and OCSP's (SP 800-57 and -78)), SP 800-131 now more broadly applies this timeline to cover these and other cryptographic functions generally - wherever used and however applied. This will have a far greater impact on large PKI's than was previously	

					planned for or even contemplated. Large PKI's will have to search their entire infrastructures and implement multiple code changes and application upgrades nearly simultaneously in order to comply. The costs to a large PKI in terms of manpower and dollars may make compliance with this broader scope impractical in the short term.	
2	DoD	DoD PKI PMO	N/A	G	In setting deadlines for compliance with the requirements in SP 800-131, consideration should be given to the following important aspects of large PKI's: 1) Dependencies on commercially available PK enablement and cryptographic functions place limitations on how quickly applications may be migrated. Several such application and product dependencies for DoD and their associated limitations are identified through out our DoD comments. 2) Component application dependencies often necessitate sequential testing and integration as one component must be upgraded before the next. In a large PKI, these dependencies have a significant impact on migration timing and schedule. 3) Implementation timelines are substantially longer for large PKI's which implement strict Quality Assurance testing after integration and functionality testing is complete. 4) Impact on End Users – With 2+ million DoD CAC user workstations, broad-based standards that affect card and credential usage will be costly and time-consuming to implement.	

3	DoD	DoD PKI PMO	N/A	T	At what point it would be desirable for relying parties to reject 80 bit security algorithms. Note that the commercial products do not easily support this feature. How much time will be allowed for making this transition?	
4	DoD	DoD PKI PMO	N/A	T	Instead of specifically referring to FIPS 140-2, use the current revision of FIPS 140, which is FIPS 140-2 at the time of writing. Also include a section on the transition from FIPS 140-2 to FIPS 140-3.	
5	DoD	DoD PKI PMO	N/A	G	DoD believes the better approach is to incorporate new algorithms into protocols that permit negotiation to the strongest, mutually acceptable algorithm, while allowing legacy products to work for a reasonable period of time. This permits early use of newer algorithms when both ends have the appropriate software while not introducing interoperability problems for legacy systems. We advocate that the DoD, like other Federal Agencies that are unable to transition to SHA-256, should be permitted to take a risk management based approach where they identify sufficiently strong compensating controls for possible SHA-1 collision scenarios.	
6	DoD	DoD PKI PMO	N/A	G, T	What industry analysis has NIST conducted to determine the readiness of COTS (Commercial Off The Shelf) products to support the transition timelines provided? **Rationale**: The DoD infrastructure utilizes and is dependent on commercial products that	

					are not yet available or in compliance with the recommendations of SP800-131.	
7	DoD	DoD PKI PMO	Section 1.2.2	E	"The CMVP has defined two classes of modes for cryptographic module operation…" is an awkward statement.	
8	DoD	DoD PKI PMO	Section 1.2.4	G	DoD disagrees with NIST's recommendation that the Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) should modify and/or revoke the accreditation certificates for already validated products and implementations which are currently valid beyond December 31, 2010. Revocation of product accreditation for implementations which are in widespread use across large scale PKI's such as the DoD's will cause insurmountable disruptions to the primary business processes which the PKI infrastructure supports and protects.	
9	DoD	DoD PKI PMO	Section 1.2.4	G	DoD would like to know under what circumstances a FIPS 140-2 rating will be invalidated and how much advance notice or time an agency will have replace the module.	
10	DoD	DoD PKI PMO	Section 2: Encryption	T	Even though the following line is at the bottom of page 11, "The authenticated encryption modes in SP 800-38 are not discussed in SP 800-131 because they use only AES, for which there are no transition issues" this SP should discuss the block cipher modes of operation (defined in SP 800-38A, 800-38B, 800-38C, 800-38D, and 800-38E) in the encryption section (perhaps just by adding a column to the table) unless all modes are allowed (unlikely).	

11	DoD	DoD PKI PMO	Section 6 Key Transport, Section 7 Key Wrapping	E	The NIST SP 800-131 specifications which prohibits the use of 2TDEA beyond 2010 seems to conflict with the "Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program" (also published by NIST in January 2010) which states that 2-key Triple DES can be used for key wrapping provided that it follow the AES Key Wrap Specification. (See page 120. The document can be found at: http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf)	
12	DoD	DoD PKI PMO	Section 7 Key Wrapping	T	Smart Card Limitation Current FIPS validated smart cards and applets do not support encryption levels higher than 2TDEA for Key Wrapping. Global Platform SCP-03 will enable AES in the future, but additional time will be needed to have these card products and applets FIPS 140 validated by NIST and tested.	
13	DoD	DoD PKI PMO	Section 8, key derivation	T	Based upon conversations with our Industry HSM Vendors we understand the following limitations exist: For key derivation, NIST 800-108 is not supported by any current HSM - CKM_ECDH1_DERIVE is not available in FIPS 140-2 mode in the Safenet Protect Server (but is available in non-FIPS mode) and the Ncipher nShield or netHSM. For Global Platform SCP01, the following key derivation methods are no longer supported in FIPS mode - CKM_DES3_DERIVE_CBC - CKM_DES3DERIVE_EBC Note, since the above key derivation	

					modes are not supported in FIPS mode, the HSM may need to be operated in non FIPS mode to support backwards compatibility. We are not aware of an official date for when support will be provided by the HSM vendors.	
14	DoD	DoD PKI PMO	Section 9, A.2	T	Secure Communications Limitation The Draft SP 800-131 should clarify that the authentication functions in SSL/TLS sessions do not require the use of 112 bit security strength, but SHA-1 is sufficient. An example is client authenticated SSL/TLS for RSA. If the use of SHA 256 were to be required for SSL/TLS authentication, applications utilizing tools such as JSSE and JCE would have to be recoded, since these tools do not currently support TLS 1.2, which is the first TLS version to enable SHA 256. OpenSSL just two weeks ago published a protocol which supports TLS v1.2; however commercial implementations have not been released yet and will require substantial testing prior to deployment.	
15	DoD	DoD PKI PMO	Section 9, A.2	T	Operating Systems Limitations Other than to implement the requirements associated with moving to higher cryptographic standards, there is no broad business need to move off of the Microsoft Windows XP platform. However, the following limitations require that operating system to be upgraded: • Microsoft Windows XP SP3 (widely deployed throughout the DoD) can support path validation but does not support	

					payload validation or Signing with SHA 256 hashes (validation only with patch). • In Windows XP SP3 environment, further investigation is required to determine if the OCSP client in use by DoD can process SHA-256 signed OCSP responses. • MS Windows Vista is not yet deployed throughout DoD. • US Gov't approved version of MS Windows 7 may not be available until May, 2010	
16	DoD	DoD PKI PMO	Section 9, A.2	T	Middleware and Operating System Limitations For SHA 256 Hashing of Secure Email We conducted a cursory review of some of the commercial products which are utilized throughout the DoD. Based on our very limited examination, the following limitations appear to exist. Further review and testing is required to confirm the validity of these potential limitations. We again recommend that NIST conduct a thorough industry survey. Supporting SHA 256 as a hashing algorithm for email digital signature with MS Outlook will require: • a mini driver (replaces the CSP) which will be supported in a future release of middleware from the DoD's primary middleware vendor (available at the end of 2010); and • an upgrade to Windows Vista SP2 or higher and MS Office 2007 or higher for both sender and recipient. Supporting SHA256 as a hashing algorithm for email digital signature with MS Exchange / Outlook Web Access will require	

					• a mini driver (replaces the CSP) which will be supported in a future release of middleware from the DoD's primary middleware vendor (available at the end of 2010) • an upgrade to Exchange 2007 or higher and Windows Vista SP2 or higher. Supporting SHA256 as hashing algorithm for email digital signature with one of the DoD approved email clients does not seem possible because there is no configuration option in that client (uses SHA1 instead). Supporting SHA256 as hashing algorithm for document digital signature appears to be possible with Adobe Acrobat Professional 9.1 and higher and a yet untested release of middleware from the DoD's primary middleware vendor. Supporting SHA256 as hashing algorithm for document digital signature with Microsoft Word / Excel appears to require upgrading to Microsoft Office 2010 (that will be released later this year). Supporting SHA256 as hashing algorithm for document digital signature with Microsoft XPS Viewer (Windows 7) does not seem possible because there is no configuration option in XPS Viewer (uses SHA1 instead). The necessary release of middleware from the DoD's primary middleware vendor is tentatively scheduled for the end of this year. Though this will include SHA-256 support in the mini driver (CSP replacement) and	

					PKCS#11 libraries, there will be other dependencies on 3rd party software that that may prevent full support for SHA-256. Currently still investigating the full impact of supporting SHA-256 with that middleware.	
17	DoD	DMDC	Section 9, A.2	T	Thorough testing will be required to confirm that there will be no adverse impact on the smart cards currently being issued and in use by DoD personnel.	
18	DoD	DoD PKI PMO	Section 10	T	Impact on Audits Use of MAC is pervasive throughout the DoD for the integrity of stored data. Data stored may have additional protections such as the operating system discretionary access controls. Upgrading DoD systems is likely to be a complex and resource-consuming endeavor. Advise and clarification is sought from NIST as to what extent the guidance regarding key sizes used in MAC apply to the stored data protection.	
19	DoD	DoD PKI PMO	Table 6	T	DoD would like to seek clarification if PKCS 1, version 1.5 for key transfer will be acceptable after 2013. If not, DoD has the following concerns: • Interoperability with Partners • Deployment of NIST schemes in cryptographic modules • Standardization of algorithm OIDs for interoperability – We would like any analysis work that has been done in this area • Lead time for encryption certificate issuance if PKCS 1.5 algorithm OID is not acceptable in the encryption certificates (relates to the previous bullet)	

From: Miles Smid [msmid@orionsec.com]

1. Although SP 800-131 mentions SP 800-57-Part 1, it does not specify its relationship to that document. It should be clarified whether the tables in SP 800-131 take precedence over the tables in SP 800-57-part 1.

2. While SP 800-57-Part 1 Table 4 provides specific date ranges for which NIST estimates that various cryptographic algorithms will be secure, the tables in SP 800-131 use vague open ended terms like "approved" or "approved beyond 2010". This makes it more difficult to plan for a transition out of an algorithm at an appropriate time. For example, by reading Table 4 of SP 800-57-part 1, the reader would know that 3TDEA was thought to be secure through 2030, but by reading Table 1 of SP 800-131, the reader only knows that Three-key Triple DES (the same algorithm) is good beyond 2010. This leads one to wonder whether NIST is backing off of its security estimate of TDEA or extending it. Since it is already 2010, the reader now has to worry that NIST might withdraw 3TDEA as soon as 2011 or never at all. The same vagueness applies to the AES algorithms in Table 1 of SP 800-131, which are only approved beyond 2010, but perhaps could be removed as soon as 2011 or never at all.

3. SP 800-131 Table 2 states that 80-bit digital signature algorithms should not be used for signature generation after 2010 but allows 80-bit signature verification to be performed indefinitely. This contradicts guidance given in Table 4 of SP 800-57-Part 1, the example b following Table 4 of SP 800-57-Part 1, and Tables 2-1 and 2-2 of SP 800-57-Part 3. The varying guidance spread over several NIST publications is, at best, confusing. If one believes that a signature algorithm can be broken and false signatures created anytime after 2010, then one would think that an open ended date on validating such signatures should be suspect. Even when signatures from 2010 and earlier are kept by the receiver in a supposedly secure location, the non-repudiation property is lost because the receiver could have modified the data and forged the signatures after 2010. Yet no rationale or guidance for accepting these signatures after 2010 is provided.

4. SP 800-131 does not consider the security life of the data being protected. It seems that data with a 20 year security life might require a significantly stronger algorithm than data with a 20 minute security life. By not emphasizing that an algorithm may have to be taken out of service well before it can be broken, users of NIST algorithms may wait to the last minute of the algorithm's security life before making a change, thus exposing previously protected data that has a long security life.

5. Table 3 of SP 800-131 approves of the ANS X9.31-1990 RNG through 2010 for new implementations and through 2015 for validated implementations. A vendor can validate this algorithm in December of 2010 and then keep selling the product through 2015. However, this standard has been withdrawn by ANSI for some

time. If NIST wants to allow this algorithm through 2015, then it should publish a description of the algorithm so that it is available for analysis.

6. NIST makes acceptations by allowing certain widely used techniques that do not meet the requirements of NIST approved algorithms. While I do not object to this practice in principle, the fact that NIST does not develop validation tests for these allowed algorithms seems to encourage vendors to implement allowed algorithms rather than approved ones and thus save the time and expense of being validated by NIST. Users operating in the *approved* mode may be unaware that the algorithm that they are using was only allowed by NIST and therefore has not been tested. NIST should develop tests for all cryptographic algorithms in the *approved* mode that could affect its security.

7. Table 4 of SP 800-131 states that SP 800-56A parameter set FA primitives and KDFs using finite fields are "approved through 2010" for new implementations and "approved through 2010 only" for already validated implementations. What is the difference between "approved through 2010" and "approved through 2010 only"?

8. In general, no rationale for the limits is provided. This leads one to wonder just how the limits are determined. Are they determined on the basis of the estimated security strengths of the algorithms, upon the size of the installed base, or upon some other factors?

From: Wade Hanniball [wade.hanniball@nbcuni.com]

Digital Cinema Initiatives, LLC

Background

This memorandum provides inputs from Digital Cinema Initiatives, LLC (DCI) regarding the Draft Special Publication 800-131, *Recommendation for the Transitioning of Cryptograp hic Algorithms and Key Sizes*.

Digital Cinema Initiatives, LLC was created in March 2002 and is a joint venture of Disney, Fox, Paramount, Sony Pictures Entertainment, Universal and Warner Bros. Studios. DCI's primary purpose is to establish and document voluntary specifications for an open architecture for Digital Cinema (DCinema) that ensures a uniform and high level of technical performance, reliability, security and quality control.[a] As a vehicle to provide DCinema requirements from the view of the above member companies, DCI developed and published the *Digital Cinema System Specification* (DCSS).[b]

Working closely with the Society of Motion Picture and Television Engineers (SMPTE), DCI has also assisted in codifying a number of specifications that define an open standard for DCinema, which have been subsequently adopted by the International Standards Organization (ISO), and together act as the sole formally standardized distribution method for DCinema throughout the world. A critical feature of this standard is assuring the security of motion picture content, and a key component of security within the standard is the physical and logical security surrounding a device in the projection booth referred to as a "Media Block." The Media Block performs content decryption, integrity validation for security messaging and content, and the provisioning of secure forensic (log) data.

The DCSS mandates that the Media Block be compliant and certified to FIPS 140-2. It has taken the industry several years to position itself to become compliant to the overall set of DCinema requirements, and in particular, FIPS 140-2 requirements. The industry is in the beginning stages of widespread adoption and rollout of the new DCinema standard, and the associated new generation of digital equipment. There is now a concern that certain changes as described in SP800-131 will disrupt this rollout, and force equipment vendors into redesign and recertification of existing products, none of which have experienced a security breach.

Cryptographic Concerns

There appear to be three issues in SP800-131 that are of concern:

1. Random number generation – The DCSS currently specifies ANSI X9.31 for symmetric content key generation (content is AES-128 encrypted for distribution).

[a] See http://www.dcimovies.com/

[b] See http://www.dcimovies.com/specification/

2. Dual key usage – SMPTE specifications use the Media Block's private key for both content Key Delivery Message (KDM) decryption and log data record message signing.

   Additionally, a Message Integrity Code (MIC) used for content integrity validation is derived within the Media Block from the decrypted content key. DCI would like to see NIST continue to discourage the use of a single key for multiple functions, but not disallow it.
3. Retirement of SHA-1 – DCinema employs both SHA-1 and SHA-256 for a variety of specified functions. DCI would like to see continuance of the restricted use of SHA-1 as currently permitted.

The DCinema environment implements a multifaceted distribution chain that includes content generation, packaging, distribution/capture, and playout. And even though the only FIPS 140-2 certified device in the chain is the Media Block, the above cryptographic concern areas impact the entire end-to-end chain, and a broad scope of entities that touch various processes along the chain. This means that many aspects of DCinema security will be impacted, as well as many globally published SMPTE specifications, in addition to the DCSS.

Discussion

DCI estimates that becoming compliant to SP800-131 in the above concern areas would take two to three years to complete. Since equipment is presently being certified and installed under FIPS 140-2, an equally critical issue is that existing and changing cryptographic constraints are not backwards compatible, given the nature of the DCinema processing chain. This presents an interoperability issue, again on a global scale. Full compliance to SP800-131 would require the modification of the DCSS, modification of standards in both SMPTE and ISO, modification of the DCI *Compliance Test Plan* (CTP)[a], redesign and production by manufacturers, recertification of all equipment, and global industry agreement on a change-over implementation period.

DCinema product manufacturers have further expressed concern over the cost of recertification at a time when significant costs have been expended in becoming initially compliant to this new set of world standards. Thus, DCI is currently of the mind that unless the existing requirements can be allowed to survive an additional two to three years beyond the pending sunset dates (end of 2010 for FIPS certification), we believe our only path is to internalize the current FIPS specifications, and devise a method to use them for the next several years.

DCI understands and supports the evolution of cryptographic processes and functions over time to maintain the necessary security advantage over potential threats. However, it is our belief that altering the DCinema specifications, standards, and tests to adhere to these three items in SP800- 131 will result in undue cost, disruption, and delay at a moment when global adoption is just starting, without providing a concrete security

[a] See http://www.dcimovies.com/compliance/

benefit. For these reasons, we are seeking a way to modify or delay these SP800-131 changes, at least for the next couple of years.

We appreciate the opportunity to provide these inputs. We would be happy to provide other contacts to DCinema industry manufacturers and participants who are just now becoming aware of SP800-131, should that be useful to your review of SP800-131 comments.